Абай атындағы Қазақ ұлттық педагогикалық университеті

ӘОЖ 378.018.43.02:004.02.056(574) Қолжазба құқығында

АДРАНОВА АСЕЛЬХАН БАГДАТОВНА

Қашықтықтан оқытудың ақпараттық қауіпсіздігін қамтамасыз етудің модельдері, әдістері және алгоритмдері

6D060200-Информатика

Философия докторы (PhD)
дәрежесін алу үшін дайындалған диссертация

Ғылыми кеңесшілер:
техника ғылымдарының докторы,
профессор Ахметов Б.С.
техника ғылымдарының докторы,
профессор Лахно В.А.

Қазақстан Республикасы
Алматы, 2020

МАЗМҰНЫ

БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

ААТБ – ақпараттық ағындарды талдау блогы;
ББ – білім базасы;
ДБ – деректер базасы;
АЖӨБ – ақпаратты жинау және өңдеу блогы;
ККБ – киберқауіпсіздік блогы;
ЖБ – жоспарлау блогы;
ЖАБ – жүзеге асыру блогы;
ВМ – *виртуалдық машина*;
ВБР – виртуалдық бұлттық ресурс;
ВБО – виртуалдық бұлттық орта;
КрҚАГ – киберқатерді анықтау графы;
ЕКГ – ескерту корреляциялық графы;
КрШХГ – кибершабуылды хабарлау графы;
ҚР МЖМБС – *Қазақстан Республикасының Мемлекеттік жалпыға міндетті білім беру стандарты*;
ҚОЖ – қашықтықтан оқыту жүйесі;
АҚ – ақпаратты қорғау;
ШКТСА – шабуыл көзі торабымен сессияны аяқтау;
АҚ – *ақпараттық қауіпсіздік;*
АББО – ақпараттық білім беру ортасы;
АТ – ақпараттық технологиялар;
АЖ – ақпараттық жүйелер;
АқЖ – ақпараттық желілер;
АКЖ – ақпараттық-коммуникациялық жүйе;
АА – ақпараттық ағын;
АМ – ақпараттық массив;
АР – ақпараттық ресурстар;
КҚ – киберқауіпсіздік;
КМКЖ – критикалық маңызды компьютерлік жүйелер;
КрҚ – киберқатер;
КрШ – кибершабуыл;
КТ – кибернетикалық тәуекел;
ШҚТ – шешім қабылдайтын тұлға;
ҚКМ – қызмет көрсету механизмі;

РЕҚЖ– рұқсат етілмеген қолжетімділік;
БЕ – бұлтты есептеулер;
АЕЖ – абонентке ескерту жіберу;
ОЖ – операциялық жүйе;
ҚҚ – қорғау құралдары;
АҚЖ – ақпаратты қорғау жүйесі;
ШГС – шабуыл графының сценарийі;
БКАЖ – басып кіруді анықтау жүйелері;
ЖҚКЖ – жаппай қызмет көрсету жүйесі;
ШҚҚЖ – шешім қабылдауды қолдау жүйелері;
ҚКҚ – қызмет көрсету құрылымы;
ДҚБЖ– деректер қорын басқару жүйесі;
АҚБЖ – ақпараттық қауіпсіздікті басқару жүйесі;
ЭҚАЖ – электрондық құжат айналымы жүйесі;
АҚС – ақпараттық қауіпсіздік саясаты;
ЖК – дербес компьютер;
БКж – *бағдарламалық-конфигурацияланатын желі;*
БӨ – бағдарламалық өнім;
ПОҚ – профессор-оқытушылар құрамы;
ҚКТ – қызмет көрсету тәртібі;
БҚЕ – бағдарламалық қамтамасыз ету;
ЖҚКТ – жаппай қызмет көрсету теориясы;
ФТ – функционалды тұрақтылық;
ДӨО – *деректерді өңдеу орталығы*;
ЖООЦББО – ЖОО-ның цифрлық білім беру ортасы;
СЖ – сараптамалық жүйелер;
DoS/DDoS – Denial of Service/ Distributed Denial of Service;

КІРІСПЕ

Зерттеудің өзектілігі: ЖОО-да жаңа цифрлық технологияларды қолданудың ұлғайып келе жатқан ауқымы, ақпараттық платформаларды және жүйелерді, атап айтқанда қашықтықтан оқыту мәселелерінде пайдалану, оқу процесіне инновациялық аппараттық-бағдарламалық құралдарды іс жүзінде жүзеге асыру, оқу орындарының ақпараттық-білім беру ортасын олардың жұмысына араласудың ұлғайып келе жатқан қиындықтары мен саны аясында осал етеді. Бұл ретте, жоғары оқу орындарының қашықтықтан оқыту жүйелерінде сақталатын және айналыстағы қорғалатын мәліметтерге мыналарды жатқызуға болады: студенттердің, оқытушылардың, ғылыми қызметкерлердің дербес деректері; оқу орнының интелектуалдық меншігін білдіретін цифрланған ақпарат; оқу процесін қамтамасыз ететін ақпараттық массивтер (мысалы, мультимедиалық контент, мәліметтер базасы, білім беру және басқа да жеке жобалау бағдарламалары және бөгде бағдарламалық өнімдер) және тағы басқалар. ЖОО-ның қашықтықтан оқыту жүйесінде аталған ақпараттық ресурстар сыртқы (ішкі) компьютерлік қаскүнемдер тарапынан ұрлау немесе бұрмалау нысаны ретінде, студенттер мен қызметкерлер тарапынан бұзақылық ниеттен болуы мүмкін.

Көптеген постиндустриялық елдерде қалыптасқан ЖОО-ның қашықтықтан оқыту жүйесіне (ҚОЖ) қолжетімділікті жаһандандыру үрдісі неғұрлым сенімді қорғау проблематикасын зерделеуге және жалпы ЖОО-ның киберқауіпсіздігінің перспективалық стратегияларын әзірлеуге байланысты маңызды мәселелерді қарастырады.

Бұл ретте бірнеше рет резервтеуге, кіріктірілген вирусқа қарсы бақылау жүйелерін және сенімділіктің жоғары деңгейі бар элементтерді енгізуге негізделген ҚОЖ-н қорғау контурын құрудың дәстүрлі әдістері жобаланатын және қолданыстағы ҚОЖ-нің техникалық-экономикалық сипаттамаларын нашарлатады. Бұдан басқа, мұндай тәсіл ЖОО-ның ҚОЖ-дегі контентті бұрмалауға немесе ауыстыруға, сондай-ақ олардың жалпы жұмысының сенімділігін қамтамасыз етуге байланысты қатерлі жағдайлардың туындау ықтималдығының қажетті азаюына әкеп соқтырмайды.

Қазіргі заманғы ЖОО-да ақпараттық-коммуникациялық технологиялар, атап айтқанда ҚОЖ оқу процесінің негізгі элементтерінің бірі. Қазіргі заманғы оқу орындары саяси және әлеуметтік саланың элементтері ретінде ақпараттық ресурстар және ақпараттық технологиялармен тікелей байланысты. Қазіргі заманғы ҚОЖ және оның ақпараттық желісінің негізгі компоненттері компьютерлік технологиялар, бұлтты технологиялар, мобильді технологиялар, ақпараттық қауіпсіздік технологиялары, деректерді өңдеудің қазіргі заманғы орталықтарының технологиялары және т.б. Олар өзара тығыз байланысты және өз кезегінде ЖОО-ның ҚОЖ-нің бағдарламалық-аппараттық кешеніне әсер етеді. Сондықтан, бір жағынан, білім алушылардың ҚОЖ-нің АТ-ресурстарына, АТ-

инфрақұрылымына барынша жылдам қол жеткізуін қамтамасыз ететін түрлі жаңа инновациялық шешімдерді енгізу қажеттілігі туындайды. Ал екінші жағынан, нақты уақытта ҚОЖ жұмысының функционалды тұрақтылығын және киберқауіпсіздігін қамтамасыз ету.

Күрделі бөлінген есептеу желілерінің ақпаратты қорғау жүйелерінің тиімділігін жоғарылату саласындағы зерттеулердің көпшілігі, оларға қашықтықтан оқыту жүйелерін, сондай-ақ киберқауіпсіздік және ақпаратты қорғау жүйелеріне қаржы ресурстарын салудың оңтайлы стратегияларын іздеу мәселесін экономикалық тұрғыдан қоюға ғана назар аударылған білім беру процесіне белсенді енгізілетін виртуалдық бұлттық технологияларды да жатқызуға болады. Бұл жұмыстар, әдетте, осындай жобалар үшін шешімдер қабылдауға және бақылау процедураларына ең озық ақпараттық технологияларды енгізуге қатысты үрдістерді ескермейді. ҚОЖ-дегі киберқатерлерге қарсы тұру үшін қарсы шараларды таңдауға жұмсалатын қаржы ресурстарын бөлу бойынша көптеген модельдердің кемшілігі - киберқауіпсіздік және ақпаратты қорғау жүйесіне қаржылық инвестициялар стратегияларын қалыптастыру бойынша нақты ұсынымдардың болмауы.

Сондықтан шешімдерді қолдаудың компьютерлік жүйелері үшін әдістер мен модельдерді дамыту бағытында жаңа зерттеулер жүргізу қажет, олар ЖОО-ның шектеулі қаржы ресурстарын бөлу бойынша, жалпы ҚОЖ-нің функционалды тұрақтылығы мен киберқауіпсіздігін құру және қолдау үшін оңтайлы стратегияларын табуға мүмкіндік береді.

Ақпаратты қорғау және ақпараттандырудың әртүрлі нысандарының ақпараттық қауіпсіздігін басқарудың тиімді жүйелерін құру мәселелерімен көптеген отандық және шетелдік ғалымдар айналысты, атап айтқанда: Б.С. Ахметов, Р.Г.Бияшев, А.В. Барабанов, Д.П. Зегжда, М.Н.Калимолдаев, С.В.Казмирчук, А.Г. Корченко, Т.С.Картбаев, В.А. Лахно, В.В. Малюков, А.С. Марков, У.А. Тукеев, M. Atighetchi, R.H. Campbell, J. Dawkins және т.б. [1-9]. Олардың зерттеулері көрсеткендей, ЖОО-ның ҚОЖ-нің рұқсатсыз қолжетімділігі мен шабуылдарға функционалды тұрақтылығын құрудың мүмкіндігімен және олардың функционалды тұрақтылығы мен киберқауіпсіздігінің қажетті деңгейін қамтамасыз ете алмайтын ЖОО-ның қашықтықтан оқыту жүйелерін қорғаудың қолданыстағы жүйелерінің тиімділігінің жеткіліксіздігі арасында айқын қарама-қайшылық бар.

Жоғарыда көрсетілген қайшылықты шешу үшін диссертацияда ғылыми мақсат қойылған, ол қолданыстағы және перспективті ақпараттық желілер негізінде ЖОО-ның ҚОЖ-н қорғалған және функционалды тұрақтылығын құрудың модельдерін, әдістері мен ақпараттық технологияларын құрудан тұрады. Сондықтан осы мәселені шешуге бағытталған диссертациялық жұмыстың тақырыбы өзекті және ғылыми және практикалық қызығушылық танытады.

Жұмыстың ғылыми бағдарламалармен, жоспарлармен, тақырыптармен байланысы: Диссертациялық жұмыс халықаралық ғылыми-зерттеу жобасында Абай атындағы ҚазҰПУ мен экономика жоғары мектебі (Мәскеу, Ресей) бірлескен «Жоғары оқу орындарының оқу процесіне цифрлық құралдардың ену мониторингі» (келісім шарт ҒЗЖ 19.04.2019ж. №19/04), «ЖОО-ларды цифрлық трансформациялаудың мақсатты және құрылымдық модельдері: базалық бағыттар мен негізгі жобалар (Абай атындағы Қазақ ұлттық педагогикалық университеті мысалында)» (келісім шарт ҒЗЖ 02.03.2020 ж. №20/03) тақырыптары аясында жүргізілді.

Зерттеудің мақсаты: ҚОЖ үшін киберқауіптерді анықтау арқылы деструктивті әсерлердің саны үнемі өсуі жағдайында ҚОЖ-н қорғау үшін пайдаланатын модельдерді, әдістерді және ақпараттық технологияларды дамыту және сәйкес қарсы шараларды таңдау.

Зерттеудің нысаны: ҚОЖ-нің функционалды тұрақтылығын қамтамасыз ету және киберқатерді анықтау процестері.

Зерттеудің пәні: ЖОО-ның ҚОЖ-нің ақпараттық қауіпсіздігін қамтамасыз ету әдістері мен модельдері.

Зерттеудің ғылыми болжамы: егер, ЖОО ҚОЖ-нің ақпараттарды қорғау және киберқауіпсіздік дәрежесін арттыру талап етілсе, онда бұл міндетті шешу ҚОЖ-і үшін ағымдағы және жаңа киберқатерлерді анықтау әдістері мен модельдерін кешенді қолдану және осы қатерлерге сәйкес келетін қарсы шараларды таңдау арқылы жүзеге асырылады.

Зерттеудің міндеттері:

− қазіргі заманғы жоғары оқу орындарының цифрлық білім беру ортасын (ЖООЦББО) және оның компоненттері-қашықтықтан оқыту жүйесінің (ҚОЖ) киберқорғаудың базалық тәсілін талдау, сондай-ақ ҚОЖ-нің виртуалдық бұлттық ресурстарының функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету бойынша мәселелерді талдау;

− ҚОЖ-нің ақпаратты қорғау жүйесін сипаттау үшін модельдерді құру;

− ҚОЖ-де киберқатерді анықтау әдісін жетілдіру;

− ҚОЖ-нің бағдарламалық-конфигурацияланатын желілері үшін виртуалдық бұлттық ресурстардың функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету үшін математикалық модельдерді жетілдіру, сондай-ақ бағдарламалық-конфигурацияланатын желілерді қолдану негізінде виртуалдық бұлттық ресурстардың функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету әдістемесін құру;

− ҚОЖ-нің киберқауіпсіздігін және ақпаратты қорғау жүйесін құрудың оңтайлы нұсқасын таңдау әдістемесін жетілдіру.

Зерттеудің әдістері: Зерттеу барысында пәндік аймақтың ерекшеліктерін және тұжырымдалған мәселелерді ескере отырып, келесі әдістер қолданылды: жүйелік талдау және күрделі жүйелер теориясы (бұл ЖОО-ның ҚОЖ-нің

иерархиялық ақпараттық желісін кездейсоқ жұмыс процесінің күйі мен ауысу графигін сипаттау үшін); ЖОО–ның ҚОЖ-нің ақпараттық желісінің функционалды тұрақтылығы мен киберқауіпсіздігінің теориялық негіздері (ҚОЖ-нің сенімділігін модельдеу үшін); сараптамалық бағалау әдістері, комбинаторлық теория және аналитикалық модельдеу (виртуалдық бұлттық ресурстардың киберқауіпсіздігін және функционалды тұрақтылығын қамтамасыз етудің математикалық моделін жетілдіру үшін); жаппай қызмет көрсету теориясы мен ойындар теориясының жалпы ережелері (ҚОЖ-нің киберқауіпсіздігін және ақпаратты қорғау жүйесін құрудың оңтайлы жолын таңдаудың әдістемелерін жетілдіру үшін).

Зерттеудің ғылыми жаңалығы:

− марковтық тізбектер негізінде ҚОЖ-нің киберқатерін сипаттау үшін модель алынды, ол ЖООЦББО және ҚОЖ-не шабуыл қатерінің нақты марковтық модельдерін құруға мүмкіндік береді және ҚОЖ-нің киберқауіпсіздігін инвестициялаудың рационалды стратегиясын таңдау алгоритмдері мен модельдерімен бірге ҚОЖ қорғалған және функционалды тұрақтылығын құру әдіснамасын жетілдіруге мүмкіндік береді;

− ҚОЖ-де киберқатерді анықтау әдісі жетілдірілді, ол қолданыстағы әдістерден айырмашылығы үлестірілген желіні өздігінен оқуға арналған рекурсивті алгоритмдерді және киберқатер түріне байланысты қарсы шараларды (стратегияларды, атап айтқанда ҚОЖ-н қорғау жағынан қаржылық немесе техникалық) таңдау;

− ҚОЖ-нің бағдарламалық-конфигурацияланатын желілері үшін ВБР-дың функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету үшін математикалық модель жетілдірілді. Бұл модельдің қолданыстағы модельдерден айырмашылығы бағдарламалық-конфигурацияланатын желілер үшін кешенді көрсеткіш негізінде мүмкін қарсы шараларды таңдау және виртуалдық бұлттық ресурстардың жағдайын ескереді, сондай-ақ виртуалдық бұлттық ортаға шабуыл графтарды қолдану процедурасы есебінен жүйенің барлық белгілі осалдықтары туралы ақпарат алуға мүмкіндік береді, сондай-ақ нақты уақыт режимінде ВБР-дың функционалды тұрақтылығы мен киберқауіпсіздігі жағдайын көрсетеді;

− ҚОЖ-нің киберқауіпсіздік және ақпаратты қорғау жүйесін құрудың оңтайлы жолын таңдау әдістемесі дамытылды, әдістеменің қолданыстағы әдістемелерден айырмашылығы, ақпараттық желіде және ҚОЖ-де киберқатерді анықтаудың жетілдірілген әдісімен, жаппай қызмет көрсету жүйесі (ЖҚКЖ) ретінде ҚОЖ-нің ақпараттық қауіпсіздігін басқару жүйесінің моделі, оқу орнының шектеулі бюджеті жағдайында ақпаратты қорғау құралдарын тиімді және ұтымды іздеу үшін антагонистік ойын моделімен толықтырылған.

Зерттеудің теориялық маңыздылығы: Компьютерлік қаскүнемдер тарапынан олардың жұмысына деструктивті араласу күрделілігінің өсуі жағдайында ҚОЖ-н қорғаудың модельдері мен әдістері одан әрі дамытылды. Бұл

ретте алғаш рет Марков тізбектеріне негізделген ҚОЖ-нің киберқатерлерін сипаттауға арналған модель алынды, ол ҚОЖ-не шабуыл жасау қатерінің нақты марковтық модельдерін құруға мүмкіндік береді. Сондай-ақ, ҚОЖ-дегі киберқатерлерді анықтау әдісі жетілдірілді, ол қолданыстағы әдістерден айырмашылығы үлестірілген желіні өздігінен оқуға арналған рекурсивті алгоритмдерден тұрады және ҚОЖ-нің бағдарламалық-конфигурацияланатын желілері үшін виртуалдық бұлттық ортаның (ВБО) функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз етуге арналған модель жетілдірілді, ол қолданыстағы модельдерден айырмашылығы ЖОО-ның бұлтты ортасының жай-күйін ескереді және бағдарламалық-конфигурацияланатын желілер үшін кешенді көрсеткіш негізінде ықтимал қарсы шараларды таңдауды жүзеге асыруға мүмкіндік береді.

Зерттеудің практикалық маңыздылығы: Rad Studio 10.3 ортасында қолданбалы бағдарламалық өнімдерді (БӨ) құру. Әзірленген БӨ ҚОЖ-нің ақпараттық қауіпсіздігін басқару жүйесін жобалау процесінің жоғары тиімділігін қамтамасыз етеді және ҚОЖ үшін қолайлы тәуекел деңгейін интерпретациялау нәтижелерінің дұрыстығын арттырады. Әзірленген бағдарламалық өнімдер негізінде жүргізілген есептеу эксперименттері диссертациялық жұмыстың негізгі теориялық маңыздылығының дұрыстығын растады. Ұсынылған шешімдер жалпы алғанда ҚОЖ-н және ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздік көрсеткішін белгілі шешімдермен салыстырғанда 12-17%-ға арттыруға мүмкіндік беретіні эксперименталды көрсетілді.

Ұсынылған әдістер, модельдер және әзірленген бағдарламалық өнімдер ЖОО-ның ҚОЖ-нің киберқорғалу дәрежесін арттыру үшін пайдаланылуы мүмкін.

Қорғауға ұсынылатын негізгі қағидалар:

− марковтық тізбектер негізінде қашықтықтан оқыту жүйесінің киберқатерін сипаттау үшін модель;

− киберқатерлер түріне байланысты қарсы шараларды таңдау және үлестірілген желіні өздігінен оқуға арналған рекурсивті алгоритмдерді қамтитын қашықтықтан оқыту жүйелерінде киберқатерлерді анықтау әдісі;

− қашықтықтан оқыту жүйесінің бағдарламалық-конфигурацияланатын желілері үшін виртуалдық бұлттық ресурстардың функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету моделі;

− қашықтықтан оқыту жүйелерінің киберқауіпсіздігін және ақпаратты қорғау жүйесін құрудың оңтайлы жолын таңдау әдістемесі.

Ізденушінің жеке үлесі. Қорғауға шығарылатын диссертацияның барлық негізгі нәтижелері ізденушімен жасалған, олардың ішінде: жоғары оқу орындарының қашықтықтан оқыту жүйесінің бағдарламалық-конфигурацияланатын желілері үшін виртуалдық бұлттық ресурстардың функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету алгоритмдері

мен модельдері; жаппай қызмет көрсету жүйесі ретінде қашықтықтан оқыту жүйесінің ақпараттық қауіпсіздікті басқару жүйесінің компьютерлік моделі.

Зерттеудің нәтижелерін сынақтан өткізу: Абай атындағы Қазақ ұлттық педагогикалық университетінің «Информатика және білімді ақпараттандыру» кафедрасының «Білімді ақпараттандыру және оқыту мәселелері» ғылыми-әдістемелік семинарында, Биоресурстарды және табиғатты пайдалану ұлттық университетінің (Украина) «Ақпараттық технологиялар» факультеттерінде, сонымен бірге халықаралық ғылыми-әдістемелік конференцияларда: «Білім берудегі ғылым мен практикадағы заманауи ақпараттық-коммуникациялық технологиялар» атты республикалық ғылыми-практикалық конференция, (Алматы, 2018); «Өнеркәсіптегі цифрлық технологиялар» атты республикалық ғылыми-практикалық конференция, (Ақтау, 2019); «Инновациялық технологиялар – ҚР-сы экономикасының кен және мұнай-газ секторларындағы іргелі және қолданбалы мәселелерді табысты шешудің кілті» атты халықаралық Сәтбаев оқулары, (Алматы, 2019); «Математикалық модельдеу мен ақпараттық технологиялар білімде және ғылымда» атты IX Халықаралық ғылыми-әдістемелік конференция (Алматы, 2020); «Безпека ресурсів інформаційних систем» атты I халықаралық ғылыми-практикалық конференциясында (Чернигов, 2020) баяндалды.

Сонымен қатар, Абай атындағы Қазақ ұлттық педагогикалық университетінің «біліктілікті арттыру және қашықтықтан білім беру» орталығына, Алматы энергетика және байланыс университетінің «Басқару жүйелері және ақпараттық технологиялар» институтында, Биоресурстарды және табиғатты пайдалану ұлттық университетінің (Украина) «Ақпараттық технологиялар» факультетінде (акт №16-34, 12.03.2020ж.) оқу процесіне ендірілді.

Жарияланымдар: Диссертация тақырыбы бойынша 14 жарияланым бар, оның 6 - ҚР БҒМ Білім және ғылым саласында сапаны қамтамасыз ету комитеті ұсынған басылымдарда, 3 мақала Scopus мәліметтер қорына кіретін басылымда, 1 мақала жақын шетелдік ғылыми конференцияда, 4 мақала халықаралық ғылыми-тәжірибелік конференция жинақтарында жарияланған.

Диссертацияның құрылымы: Диссертациялық жұмыс, кіріспеден, үш тараудан, қорытындыдан, пайдаланылған әдебиеттер тізімінен және қосымшалардан тұрады.

Кіріспеде зерттеудің ғылыми аппараты ұсынылған, зерттеу тақырыбының өзектілігі, оның теория мен практикада әзірлену деңгейі ашылған, зерттеу проблемасының негізінде қарама-қайшылықтар тұжырымдалды, зерттеудің мақсаты, нысаны, пәні, ғылыми болжамы, міндеттері, әдістері анықталады, зерттеудің ғылыми жаңалығы, теориялық және практикалық маңыздылығы ашылған, қорғауға ұсынылатын негізгі қағидалар қарастырылған.

Бірінші тарауда онлайн-білім беру модельдеріне талдау жасалған, ақпараттың қол жетімділік, пайдалану қарапайымдылығы, параметрлер

икемділігі, оқу контентін басқару, пайдаланушыларды басқару, пайдаланушылар арасындағы қарым-қатынас, статистика және есебі, құны және лицензиялық саясат өлшемдері бойынша бағаланатын ҚОЖ-нің ең танымал жүйелері қарастырылған. Сондай-ақ қашықтықтан оқытуды ұйымдастырудың әртүрлі бұлтты-бағытталған тәсілдері сипатталған. Қызметтер мен ресурстар тұрғысынан жоғары оқу орындары үшін «академиялық бұлтты» пайдаланудың артықшылығы негізделеді, ол құрылымы мен орналасуы экономикалық тұрғыдан мүмкін болатындай қамтамасыз етуі керек. ЖОО қашықтықтан оқыту жүйелеріндегі ақпараттық ағындарды ұйымдастыру құрылымы ұсынылған, ол қашықтықтан оқыту жүйесінде айналымдағы ақпараттық ағындарды бақылау мен өңдеудің қазіргі және жаңа перспективалы механизмін кешенді өзара әрекеттесу тиімділігін арттыруға қабілетті. ЖОО-ның қашықтықтан оқыту жүйесінде қолданылатын, виртуалдық бұлттық ресурстар мәселелерінің функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету сұрақтары зерттелді. Ақпараттандырудың әртүрлі нысандарының ақпаратты қорғау жүйесіне және киберқауіпсіздігіне, оның ішінде ЖОО-н қашықтықтан оқыту жүйесіне инвестициялаудың тиімділігін бағалау үшін қолда бар модельдерге талдау жасалды.

Екінші тарауда Ақпараттық желілер мен қашықтықтан оқыту жүйелеріне шабуылдардың қаупін сипаттайтын, көрсеткіштер үшін ақпаратты қорғау жүйелерін сипаттау бойынша мәселелерді шешу моделі алынды. ҚОЖ-де және ақпараттық желідегі киберқатерді анықтаудың жетілдірілген әдісі ұсынылған, ол қолданыстағы әдістерден айырмашылығы үлестірілген желіні өздігінен оқуға арналған рекурсивті алгоритмдерді және киберқатер түріне байланысты қарсы шараларды (стратегияларды, атап айтқанда ҚОЖ-нің ақпараттық желісін қорғау жағынан қаржылық немесе техникалық) таңдау. ҚОЖ-нің бағдарламалық-конфигурацияланатын желілері үшін виртуалдық бұлттық ресурстардың (ВБР) функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету үшін жетілдірілген модель сипатталған. Модель виртуалдық бұлттық ортаға кибершабуыл параметрлерінің әсерін есепке алу есебінен жетілдірілген. Сондай-ақ модельде бағдарламалық-конфигурацияланатын желілер үшін кешенді көрсеткіш негізінде мүмкін қарсы шараларды таңдау және виртуалдық бұлттық ресурстардың жағдайын ескереді. Бұлттық ортада қатерлерді талдау үшін алгоритмдер әзірленді, жұмыстың нәтижесі виртуалдық бұлттық ортаға шабуыл жасаудың бір немесе бірнеше жолын алу; қарсы шараларды таңдау, жұмыс нәтижесі қашықтықтан оқыту жүйесіне және оның виртуалдық бұлттық ресурстарына шабуылдың нақты сценарийі үшін қарсы шараны таңдау. Әзірленген әдістеме мен модельдерге эксперименталды апробация жүргізілді. Алынған нәтижелердің адекватылығын растау үшін тестілік виртуалдық бұлттық орта іске асырылды. Ұсынылған шешімдер жалпы алғанда ҚОЖ-н және ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздік көрсеткішін белгілі

шешімдермен салыстырғанда 12-17%-ға арттыруға мүмкіндік беретіні эксперименталды көрсетілді.

Үшінші тарауда қашықтықтан оқыту жүйесінің ақпараттық қауіпсіздікті басқару жүйесін ЖҚКЖ ретінде бейнелеудің ұқсастығы анықталған. Бұл қашықтықтан оқыту жүйесі мен жаппай қызмет көрсету жүйесінің арасындағы құрылымдық және функционалды ұқсастықтарын анықтаудың арқасында мүмкін болды. Жаппай қызмет көрсету жүйесінің параметрлерін анықтау үшін модельдер одан әрі дамытылды, ол құрылымдық, мазмұндық, функционалды ұқсастықтар есебінен ЖОО-ның қашықтықтан оқыту жүйелері үшін ақпараттық қауіпсіздікті басқару жүйесінің көптеген сандық сипаттамаларын қалыптастыруға мүмкіндік береді және де ол компьютерлік қаскүнемдер тарапынан қашықтықтан оқыту жүйесіне деструктивті әсерлердің саны мен күрделілігінің өсу перспективаларын ескере отырып, жоғары оқу орындары үшін ақпараттық қауіпсіздікті басқару жүйесін жобалау процесінің тиімділігін қамтамасыз етуге мүмкіндік береді. Есептеу эксперименттері жүргізілді, олар негізгі теориялық ережелер мен практикалық зерттемелердің дұрыстығын растады.

ҚОЖ-нің киберқауіпсіздік және ақпаратты қорғау жүйесін құрудың оңтайлы жолын таңдау әдістемесі одан әрі дамыды, әдістеменің басқаларынан айырмашылығы, ақпараттық желіде және ҚОЖ-де киберқатерді анықтаудың жетілдірілген әдісімен, ЖҚКЖ ретінде ҚОЖ-нің ақпараттық қауіпсіздігін басқару жүйесінің моделімен, оқу орнының шектеулі бюджеті жағдайында ақпаратты қорғау құралдарын тиімді және ұтымды іздеу үшін антагонистік ойын моделімен толықтырылған.

Қорытындыда диссертациялық зерттеудің теориялық және практикалық нәтижелерін жинақтай келе, қорғауға шығарылатын ережелердің дұрыстығын растайтын негізгі қорытындылар жасалды.

1 ЖОО-НЫҢ ҚАШЫҚТЫҚТАН ОҚЫТУ ЖӘНЕ БҰЛТТЫҚ ЕСЕПТЕУ ЖҮЙЕЛЕРІНІҢ КИБЕРҚАУІПСІЗДІК СТРАТЕГИЯСЫНЫҢ ҚҰРАМДАС БӨЛІКТЕРІН ТАЛДАУ

1.1 Қашықтықтан оқытудың заманауи технологиялары

XXI ғасырдың басында әлемнің көптеген дамыған елдерінде қалыптасқан дәстүрлі білім беру жүйесі түбегейлі реформалауды қажет ететіні айқын болып отыр. Бұл, атап айтқанда, ол өзгермелі және қарқынды дамып келе жатқан әлемде адамзаттың өмір сүруінің жаңа шарттарына сәйкес келмейтіні және өркениетті одан әрі дамыту үшін тежеуіш бола алатындығымен байланысты.

Тығырықтан шығудың принципті мүмкіндігі білім беру жүйесіне: өзге мақсатпен және түбегейлі өзге контентпен сапалы өзге тәсілдерді жасау болып табылады. Әрине, мұндай жүйе қашықтықтан білім беру мүмкіндігін де болжауы тиіс.

Бүгін біз төртінші өнеркәсіптік революцияның бастауында тұрмыз. Ол шетелде жаңа мыңжылдықтың тоғысында басталды және цифрлық революцияға сүйенеді. Оның негізгі ерекшеліктері – бұл «барлық жерде жүретін» және мобильді Интернет, шағын өндірістік құрылғылар (олар үнемі арзандауда), жасанды интеллект жүйелері, оқыту машиналары және технологиялар.

Аппараттық және бағдарламалық қамтамасыз етуге, жергілікті және жаһандық желілерде негізделген білім беруді цифрландыру жаңалық болып табылмайды, бірақ экономиканың жаһандануы жағдайында қоғамның трансформациясын туындай отырып, неғұрлым жетілдірілген және интеграцияланған болып келеді.

Қазіргі заманғы цифрлық технологиялар бүкіл әлемдегі жоғары оқу орындары мен басқа да білім беру мекемелерін дамыту үшін жаңа құралдар ұсынады. Бұл жоғары оқу орындарының жұмыс істеу шарттарының, олардың жұмысын ұйымдастыруға және пайдаланылатын білім беру технологияларына көптеген дәстүрлі тәсілдерді қайта қарау және дамыту қажеттілігін туындататын жаһандық өзгерістерге алып келеді.

Білім беру қызметтерінің жаһандық нарығында ұстанымдарды сақтау және күшейту мақсатын қойған жоғары оқу орындарының алдында халықаралық ғылыми-білім беру кеңістігіне кіру міндеті тұр. Жоғары оқу орындарының стратегиялары арасында - цифрлық жоғары оқу орнын құру, оның ажырамас бөлігі қашықтықтан білім беруге арналған қызметтер мен тиісті контент болып табылады.

Бұл міндеттер «Білім туралы» заңында, жоғары білім берудің мемлекеттік жалпыға міндетті стандарттарында (ЖББ МЖМС) ерекше назар аударылады. Жоғары білім берудің мемлекеттік жалпыға міндетті білім беру стандарттарында жүзеге асырылған құзыреттілік тәсіл цифрлық қоғамның әлеуметтік-кәсіптік ұтқырлығы, тұрақты кәсіби өсу жағдайында талап етілетін студенттердің білімін,

іскерлігін, қабілеті мен құзыреттілігін қалыптастыру бойынша өсіп келе жатқан талаптарды көрсетті.

Жоғары оқу орындарының ақпараттық-білім беру ортасын дамытуға қойылатын тиісті талаптар да өзгереді, атап айтқанда, қашықтықтан білім беру технологиялары мен электрондық оқытуды қолдану мүмкіндіктері кеңейтілді, білім беру ресурстарына, оның ішінде ақпараттық-телекоммуникациялық интернет желісінің мүмкіндіктерін пайдалана отырып қол жеткізу бойынша шарттар нақтыланды. Бірнеше білім беру ұйымдарының, оның ішінде шетелдік ұйымдардың білім беру ресурстарын жоғары тиімділікпен қамтамасыз ете алатын білім беру бағдарламаларын жүзеге асырудың желілік нысандары мен технологияларына көп көңіл бөлінеді. Педагогикалық жоғары оқу орны жағдайында білім беру процесін ұйымдастыру және ғылыми-педагогикалық кадрлардың біліктілігін арттыруды ұйымдастыру үшін бірыңғай білім беру ортасын пайдалану корпоративтік білім беру идеялары мен желілік тәсіл негізінде жоғары білім берудің мемлекеттік жалпыға міндетті білім беру стандарттарында анықталатын құзыреттерді қалыптастырудың тиімді құралы болып табылады.

Жоғарыда аталғандай оқытушылар мен білім алушылардың қарым-қатынасын дамыту үшін «Цифрлық университет» шеңберінде қашықтықтан білім беру технологиялары мен жүйелерін әзірлеу және енгізуге байланысты міндеттер де өзекті болып қалуда. Қашықтықтан оқыту технологиялары оқу ақпаратына интерактивті қолжетімділіктің және оқыту траекториясын басқарудың түрлі деңгейлерін пайдаланады, бұл тұлғалық-бағдарлы оқыту идеологиясын жүзеге асыруға ықпал етеді. Көптеген қазіргі заманғы жоғары оқу орындарында LMS Moodle немесе соған ұқсас қашықтықтан оқытуды басқару жүйесі енгізілді немесе белсенді жүзеге асырылуда.

Қашықтықтан білім беруде цифрлық технологияларды қолданудың қосымша бағыты цифрлық кітапханалардың дамуы болды. Цифрландыру арқасында бүгінде әркім бұрын сарапшылар мен ғалымдар үшін ғана қол жетімді болатын ақпаратқа қол жеткізе алады.

Жоғарыда аталған міндеттерді шеше отырып, қазіргі заманғы жоғары оқу орнының қашықтықтан білім беру жүйесіндегі ақпаратты қорғауға байланысты, параллельді тапсырма туралы есте сақтау қажет.

Ақпараттық және телекоммуникациялық технологиялардың қарқынды дамуы ақпараттық білім беру ортасын өзгертеді, оның шеңберінде оқыту процесі жүзеге асырылады. Әлемдік тенденциялар болашақта синхронды, асинхронды, қашықтықтан және аралас оқыту сияқты онлайн-білім берудің (eLearning) икемді модельдерімен болатындығын көрсетеді.

1. Синхронды оқытудың үлгісі вебинарлар бола алады, ол оқытушы мен студенттер арасындағы қарым-қатынас нақты уақытта болған кезде жүреді. Вебинарларда ақпаратты жіберуге және алуға ғана емес, сонымен қатар пікірталастар, сауалнама, брейнсторминг өткізуге де болады. Мұндай сабақ

дәстүрлі сабақты еске түсіреді, жалғыз маңызды айырмашылығы-оқытушы студенттердің жағдайын бағалай алмайды.

2. *Қашықтықтан оқыту* (distance learning) – студент нақты уақытта мұғаліммен байланыс жасамайтын, бірақ онымен қашықтықтан электрондық пошта, скайп және т.б. арқылы байланысатын әдіс.

3. *Асинхронды оқыту* – қашықтықтан оқыту әдісі, оның барысында студенттер оқытушымен байланыс орнатпайды, бірақ электронды курстар, блогтар, CD және т.б. курстарын оқиды.

4. Әсіресе, оқу процесінде *аралас оқыту* технологияларын қолдану перспективалы, ол қашықтықтан оқыту технологияларының мүмкіндіктерін дәстүрлі оқыту формаларының артықшылықтарымен біріктіреді. Студент оқу материалының бір бөлігін өз уақытын, орнын белгілей отырып онлайн меңгереді, ал материалдың басқа бөлігін ЖОО аудиторияларында оқиды.

«Аралас оқытудың» негізгі модельдері 1- суретте көрсетілген[10].

4.1 «айналдыру» моделі - бұл модельдің ерекшелігі, ол:

– студенттер белгілі бір уақыт аралығында әртүрлі оқу «станциялары» арасында аудиторияда қозғалады;

– ең болмағанда бір шағын топ тапсырмаларды онлайн режимде орындауы керек, басқалары – бірігіп жұмыс істеу тиімді болуы үшін қағаз бен қарындаштар немесе басқа құралдарды қолдана отырып белгілі бір жоба бойынша жұмыс жасайды;

– студенттер сабақ барысында барлық «станциялардан» өтуі керек.

4.1.1 Жұмыс аймақтарын «айналу» (Station Rotation) – студенттер бір немесе бірнеше (көп емес) аудитория ішінде әртүрлі «станциялар» арасында ауысып отыратын курсты немесе пәнді ұйымдастыруға арналған модель.

4.1.2 Зертханалардың «айналуы» (LabRotation) – оқу курсын ұйымдастыру моделі, «станциялардың» бірі компьютерлік зертханада өтеді, онда студенттер өздігінен онлайн режимде оқиды.

4.1.3 «Ауыстырылған класс» (FlippedClassroom) моделі – студенттер уақытын және оқу қарқынын өз бетінше басқара отырып, теориялық оқу материалын үйде оқиды, ал аудиторияда олар материалды тереңірек меңгеру үшін талқылайды. Оқытушы тек фасилитатор рөлін атқарады, осылайша даулы мәселелерді шешуге көмектеседі.

4.1.4 Жеке «айналу» (IndividualRotation) – бұл араласқан оқыту моделі, онда әр білім алушының жеке кестесі бар және оның әр қолжетімді «станцияға» баруы міндетті емес. Кесте автоматты түрде жасалады (егер университетте қажетті бағдарламалық жасақтама болса) немесе оқытушы жасайды.

Сурет 1 – «Аралас оқытудың» негізгі модельдері

4.2 Икемді модель (FlexModel) – белгілі бір әрекет офлайн режимде өтсе де, онлайн-құраушы студенттерді оқытудың негізі болып табылатын оқыту курсы. Студенттер әртүрлі оқыту форматтарынан тұратын жеке, икемді кесте бойынша жұмыс істейді. Оқытушы кез-келген кеңестерге қолжетімді және студенттер негізінен университет аудиторияларында оқиды және жеке үй тапсырмасын орындайды.

4.3 Өздігінен араластыру моделі (LaCarteModel) – студент курсты толығымен онлайн режимде өтеді және университеттегі немесе оқу орталығындағы сабақтарға қатысады. Бұл модельде оқытушы онлайн-оқытушы. Білім алушылар онлайн-курсты оқу орнында (егер жабдықтар мен аудиториялар мүмкіндік берсе) немесе үйде оқи алады. Бұл модельді барлық оқу пәндеріне қолдануға болмайды, себебі онлайн курстар университетте топпен және оқытушымен өтетін пәндермен араластырылуы керек (әлеуметтік аспект).

4.4 Виртуалдық оқытудың байытылған моделі (EnrichedVirtualmodel) – бұл курс моделінде студенттер оқытушының қатысуымен курстың бір бөлігін офлайн режимде (бетпе-бет) өткізіп, содан кейін жеке тапсырмаларды өздері орындауы керек. Онлайн-оқыту студенттерді оқытудың негізі болады, әсіресе студенттер университеттің аудиторияларынан алыста болған жағдайда, оқу пәнінің оқытушысы, әдетте, онлайн және офлайн режимде жұмыс істейді.

Қашықтықтан оқытудың барлық жүйелерін (ҚОЖ, LMS – Learning Management Systems) ақпаратқа қол жетімділік, пайдалану қарапайымдылығы, баптау параметрлерінің икемділігі, оқу контентін басқару, пайдаланушыларды басқару, пайдаланушылар арасындағы қарым-қатынас, статистика және есептілік, құны және лицензиялық саясат өлшемдері бойынша бағалауға болады.

Жоғары технологиялар мен интернет желісінің дамуымен стандартталған білім беру тоқтады. Жастар жиі саналы түрде түрлі онлайн-платформаларды,

курстар мен вебинарларды қолдана отырып, қашықтықтан білім алуды таңдайды. Нарық өсіп келе жатқан сұранысқа жауап береді және бүкіл әлемде ақылы және ақысыз негізде ірі ресурстар пайда бола бастады. Сонымен қатар, Гарвард және Йель сияқты Плющь лигасының университеттері түрлі платформаларда гуманитарлық және нақты ғылымдар бойынша арнайы курстарды ұсынады.

Білім алу әлемнің кез-келген нүктесінен қолжетімді, тек тұрақты интернет байланысы қажет. Жалпы алғанда, онлайн-оқытудың инновациялық әдісі ақпарат арналарын кеңейтуге ұмтылатын, нақты дағдыларын арттырғысы келетін және баға мәселесіне мұқият қарайтын қазіргі заман адамдарының ойлау механикасына бейімделген, себебі онлайн білім алуға университет қабырғасында жүріп толыққанды диплом алғаннан гөрі аз қаражат кетеді.

Қашықтықтан оқыту жүйесін құру процесі төрт кезеңнен тұрады:

- техникалық жабдықтарды орнату және баптау,
- бағдарламалық жасақтаманы орнату,
- студенттер мен оқытушылардың аккаунттарын баптау,
- жүйенің ресурстары мен сервистеріне дербес қол жеткімділікті қамтамасыз ету.

Мазмұндық компонент студенттердің аккаунттарына арналған мәліметтерден және виртуалдық жұмыс үстелінің мәліметтерінен тұрады. Кірісте жүйеге келу керек келесі мәліметтерге білім алушыға қолжетімділікті қамтамасыз ету қажет: студенттердің жеке мәліметтері, оқу пәндерінің тізімі, бағдарламалық қамтамасыздандыру пакеті, кіруге мүмкіндік беретін ресурстар мен қызметтер тізімдері. Осы мәліметтерді жүйе қолданушыларының мәліметтер қорына енгізу арқылы осы кезеңде цифрлық контент алуға болады: бағдарламалық платформаларға қол жеткізудің белгіленген деңгейі бар пайдаланушылардың деректер базасы, виртуалдық жұмыс үстелі, ол студенттерді бағдарламалық платформалармен және пакеттермен оқыту үшін қажетті әр студентке қалыптастырылады.

Қашықтықтан оқытудың дұрыс ұйымдастырылған жүйесінің нәтижесі істен шығуға төтеп бере алатын бағдарламалық-техникалық инфрақұрылым (серверлер, деректер қоймасы, жергілікті желі және оларға қол жеткізу үшін Интернет) болуы тиіс, ол барлық қажетті ресурстарды орналастыруды және студенттердің осы ресурстар мен сервистерге тиімді қол жеткізуін қамтамасыз етеді [11,13-16].

Сипатталған ортаны ұсыну нысаны техникалық және бағдарламалық деңгейде «академиялық бұлт» қасиеттеріне сәйкес келетін цифрлық білім беру ортасының бұлтқа негізделген бағдарламалық және аппараттық инфрақұрылымы болып табылады.

Айта кету керек, «бұлттар» қызмет етуге қойылатын

- масштабталу;
- икемділік;
- тәуелсіз меншік;

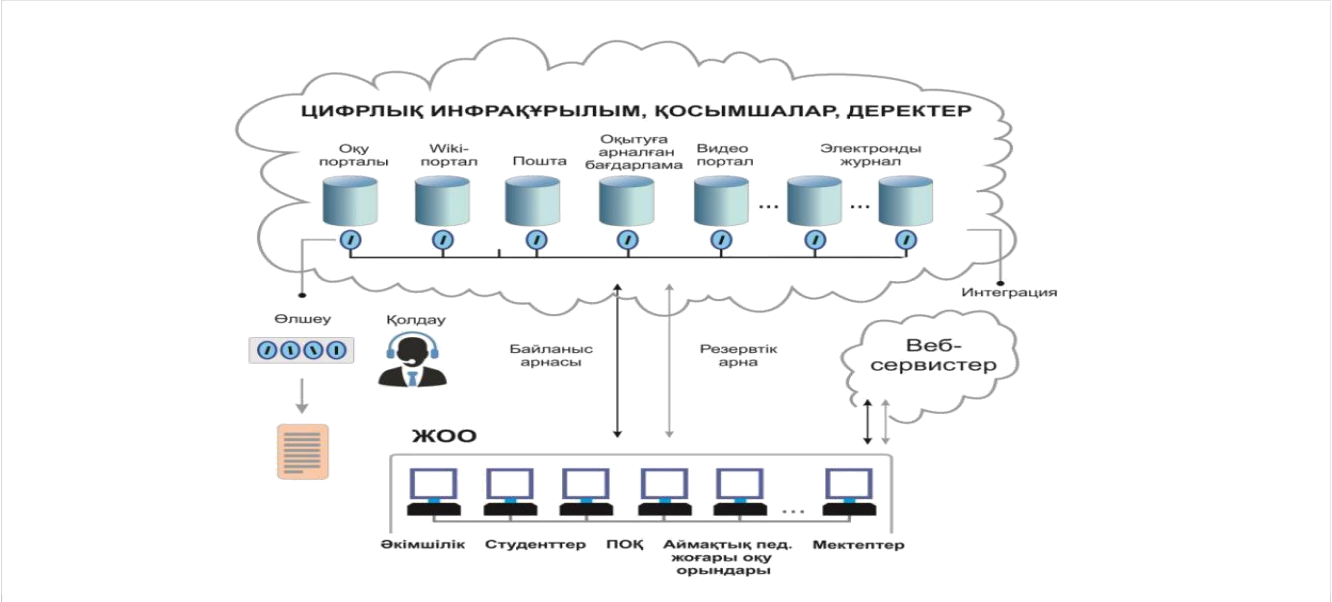
– пайдаланылған ресурстар үшін төлем;

– өзіне-өзі қызмет көрсету секілді талаптарды нақты қанағаттандыруы керек.

Бюджеті шектеулі ЖОО-ы үшін «академиялық бұлт» құру мүмкіндігі бар, оның ерекшелігі бұл жүйені университеттің өзінде де орнатуға болады және сыртқы бұлттық қызмет провайдерлерінің дайын ресурстарын алуға болады (білім беру үшін корпоративтік шешімдер деп аталатын) немесе арнайы білім порталдарының (қашықтықтан оқыту орындары) ресурстарын қолдана аласыз және жетілдіре аласыз, бірақ сонымен қатар тиімділік, оқу орнының ауқымы және т.б. кейбір факторларды басшылыққа алу керек.

Университеттің «академиялық бұлты» – бұлттың есептеу технологиялары негізінде жүзеге асырылатын техникалық, бағдарламалық және технологиялық, ақпараттық ресурстар мен қызметтердің жиынтығынан тұратынжәне жергілікті желі мен Интернетті қолдану арқылы университет студенттерінің оқу іс-әрекеттерін қамтамасыз ететін жоғары оқу орнының бұлтқа бағытталған ортасы.

Мысал ретінде 2–суретте Абай атындағы Қазақ ұлттық педагогикалық университетінің «академиялық бұлт» құрылымы көрсетілген.



Сурет 2 – «Академиялық бұлт» құрылымының моделі

Бұл шешімді таңдауда келесі мәселелерге назар аударылды.

«Академиялық бұлт» әр академиялық пәнге электронды оқу ресурстары мен қызметтерінің толық спектрін, атап айтқанда, электронды оқу курсын, электронды оқулық, оқып-үйрету бейнесін, баспа құралдарының толық мәтінді электронды көшірмелерін, ұжымдық жұмысқа арналған құралдарды, онлайн байланыс құралдарын және виртуалдық зертханалық сабақтарды қолдауды қамтамасыз етуі керек. Академиялық бұлт студенттерге оқу процесінде қолданылатын

бағдарламалық өнімдерге қол жетімділікті қамтамасыз етеді, мысалы, бағдарламалау, модельдеу, болжау, жобаларды басқару, математикалық және статистикалық орталарға, геоақпараттық жүйелерге және т.б. «Академиялық бұлттың» жұмыс істеуін қамтамасыз ететін бағдарламалық және технологиялық платформалар қолданушыларға бір ортадан кіруді, көрсетілетін қызметтердің санын уақыт пен ресурстар көрсеткіштері бойынша өлшей алуды, қолданушы сұранысы бойынша қызмет көрсетуді, желіге ауқымды қол жетімділікті қамтамасыз етуі керек, сонымен қатар ресурстарды біріктіретін және икемді таратын қажетті құралдары болуы керек.

«Академиялық бұлт» құрылымы. Егер «академиялық бұлтты» құру үшін құрылымдық тәсіл қолданылса, онда оның мынандай бес негізгі деңгейін атауға болады: физикалық, виртуализациялау, виртуалдық ресурстарды басқару, платформа деңгейі және бағдарламалық жасақтама деңгейі.

Ұсынылған «академиялық бұлт» моделі университеттің өз инфрақұрылымы базасында, IaaS моделі бойынша бұлттық инфрақұрылымды жалға алу негізінде орнатыла алады. Бұл жағдайда, университеттің сұрауы бойынша қажетті динамикалық ресурстар (есептеу және сақтау), виртуалдық серверлер, желілік инфрақұрылым беріледі. Немесе екінші жағдайда PaaS моделі бойынша, операциялық жүйелерді, ДҚБЖ, коммуникациялық бағдарламалық жабдықтарды, компьютерлік желілерді, серверлерді, мәліметтер қоймаларын қоса алғанда, барлық ақпараттық технологиялық инфрақұрылымды провайдер қамтамасыз етеді және басқарады, сонымен қатар қолжетімді платформалардың жиынтығын және платформаның басқарылатын параметрлерін де провайдер анықтайды. Таңдаған орналастыру нұсқасына байланысты «жеке бұлт» типінде өз инфрақұрылымыңызды құрудың немесе ақпараттық технологиялар саласындағы компаниялардан IaaS не PaaS модельдері бойынша жалға алынған платформалардың құнын бағалауға болады.

Жоғары оқу орнының цифрлық білім беру ортасының (ЖОО ЦББО) құрылымын талдау қорғаныс тарапының назарын ақпараттық қауіпсіздік (АҚ) және киберқауіпсіздік (КҚ) жоспарындағы неғұрлым тар учаскелерге шоғырландыруға, сондай-ақ ЖОО ЦББО-н қорғаудың тиімді контурын құруға бағытталған ресурстардың (ұйымдастырушылық, техникалық, қаржылық) шығындарын оңтайландыруға мүмкіндік береді.

Соңғы онжылдықтарға тән ақпараттық-коммуникациялық технологиялар жетістіктерін енгізудің жалпы әлемдік үрдісі «ақпараттық қоғам» үшін қоғамдық және өндірістік қарым-қатынастарды пайдаланудың және нығайтудың мәдениетін қалыптастыру қарқынынан елеулі басымдыққа ие болып, киберқауіпсіздікті қамтамасыз ету бірінші кезектегі мәселеге айналуына байланысты бұл Қазақстанда да қолдауға ие болып отыр[12].

Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны») Қазақстанның әлемнің ең дамыған 30 мемлекетінің қатарына енуі бойынша

«Қазақстан-2050» Стратегиясының тәсілдерін ескере отырып, Қазақстан Республикасы Президентінің «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» атты Жолдауына сәйкес әзірленді.

Тұжырымдама мемлекеттік органдарды ақпараттандыру, мемлекеттік көрсетілетін қызметтерді автоматтандыру, «цифрлы» экономиканы дамыту және өнеркәсіптегі өндірістік процестерді технологиялық жаңғырту перспективалары, ақпараттық-коммуникациялық қызметтер көрсету аясын кеңейту саласындағы ағымдағы ахуалды бағалауға негізделген.

Тұжырымдама электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникация желілерін қорғау, ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалануды қамтамасыз ету саласындағы мемлекеттік саясатты іске асырудың негізгі бағыттарын белгілейді.

Ақпараттық қауіпсіздік мәселелері қалыптасқан кезеңнен бастап бар ақпараттың сипатын ескере отырып, көпшілікке қолжетімді және құпия электрондық ақпараттық ресурстар мен жүйелердің құқықтық режимдері сараланды, меншік иелерінің, оларды қорғау жөніндегі иеленушілер мен пайдаланушылардың құқықтары мен міндеттері белгіленді.

Мемлекеттік органдар және ақпараттандыру мен байланыс саласындағы ақпараттық қауіпсіздікті қамтамасыз ету бойынша басқа да субъектілердің қызметі олардың салалық құзыретіне, сондай-ақ АКТ пайдаланумен байланысты нысаналы салалардағы байланысты және ақпараттық технологияларды реттеу, жеке деректерді қорғау, мемлекеттік құпияларды қорғау, шетелдік техникалық барлау қызметіне қарсы іс-қимыл, байланыс желілеріндегі жедел-іздестіру қызметі, АКТ пайдалану арқылы жасалатын қылмыстарды тергеу және басқалары) мақсаттары мен міндеттеріне сәйкес жүзеге асырылады.

Тұтастай алғанда, ғаламдық бәсекелестік жағдайларында электрондық ақпараттық ресурстардың, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қауіп-қатерлерден қорғалу деңгейіне қол жеткізу және сол деңгейде ұстау болып табылады.

1.2 Киберқауіпсіздікті қамтамасыз ету қажеттілігін ескере отырып, қашықтықтан білім беру жүйесінің ақпараттық ағындарын талдау

Цифрлық саладағы кәсіпорындардың ақпараттық қауіпсіздігі мен киберқауіпсіздігін қамтамасыз ету проблематикасымен айналысатын көптеген авторлар, соның ішіне қашықтықтан оқыту жүйелерін да жатқызуға болады, олар қашықтықтан оқыту жүйесінің ішіндегі ақпараттық ағындарды басқару жүйесі осы ағындардың қызмет ету мақсаттарын, сондай-ақ әрбір ағыннан тұратын контентті бөлуге негізделген тәсіл ең нәтижелі болуы мүмкін екенін көрсетті [17].

Осылайша, диссертациялық жұмыстың осы тарауының бөлігі шеңберінде жекелеген ақпараттық ағындарының қорғалу дәрежесін ескеретін, қашықтықтан оқыту жүйесінің құрылымын құру бойынша міндеті, сонымен қатар, ақпараттық

ағынға бақылауды қамтамасыз етуге қабілетті болатын, сондай-ақ қашықтықтан оқыту жүйесін компьютерлік қаскүнемдер тарапынан келетін еркін ақпараттық шабуылдардан қорғауды қарастырамыз.

Қашықтықтан оқыту жүйелері үшін және басқа да көптеген цифрлық жүйелер үшін, белгілі бір дәрежеде білім алушылардың дайындық деңгейіне, сондай-ақ жалпы қашықтықтан оқыту жүйесінің жұмысқа қабілеттілігіне әсер ете алатын негізгі қатерлердің екі түрін бөліп көрсетуге болады. Басқа авторлардың [18–24] көптеген зерттеулерінде нақты толық классификациясыз қатерлердің топтары қарастырылған, оларға жатқызуға болады:

– сыртқы қатерлер, атап айтқанда қаскүнемнің қашықтықтан оқыту жүйесіне қашықтықтан әсер ету, мысалы, қашықтықтан оқыту жүйесіне заңсыз кіру үшін мүмкіндіктер жасауға бағытталған;

– ішкі қатерлер, бұл қаскүнемдердің қашықтықтан оқыту жүйесіне, осалдықтар мен оны қорғау контурындағы әлсіз жерлерді пайдалана отырып, бөгде ақпараттық ағындарды заңсыз енгізуі мүмкін.

Қашықтықтан оқыту жүйесінің негізгі миссиясын жүзеге асыруға, атап айтқанда барлық студенттерге олардың орналасқан жеріне, экономикалық әлеуметтік және басқа да жағдайларға қарамастан, сапалы білім алуға мүмкіндік беруге, сонымен бірге тиімді және бәсекеге қабілетті болуына мүмкіндік беру керек. Қазіргі ЖОО-ның кез келген қашықтықтан оқыту жүйесі келесі қасиеттерге ие болуы тиіс:

– қашықтықтан оқыту жүйесіндегі айналымдағы ақпараттық ағындарды сапалы және жедел өңдеу;

– қашықтықтан оқыту жүйесі жұмысының үздіксіз және тұрақты цикліне ықпал ету;

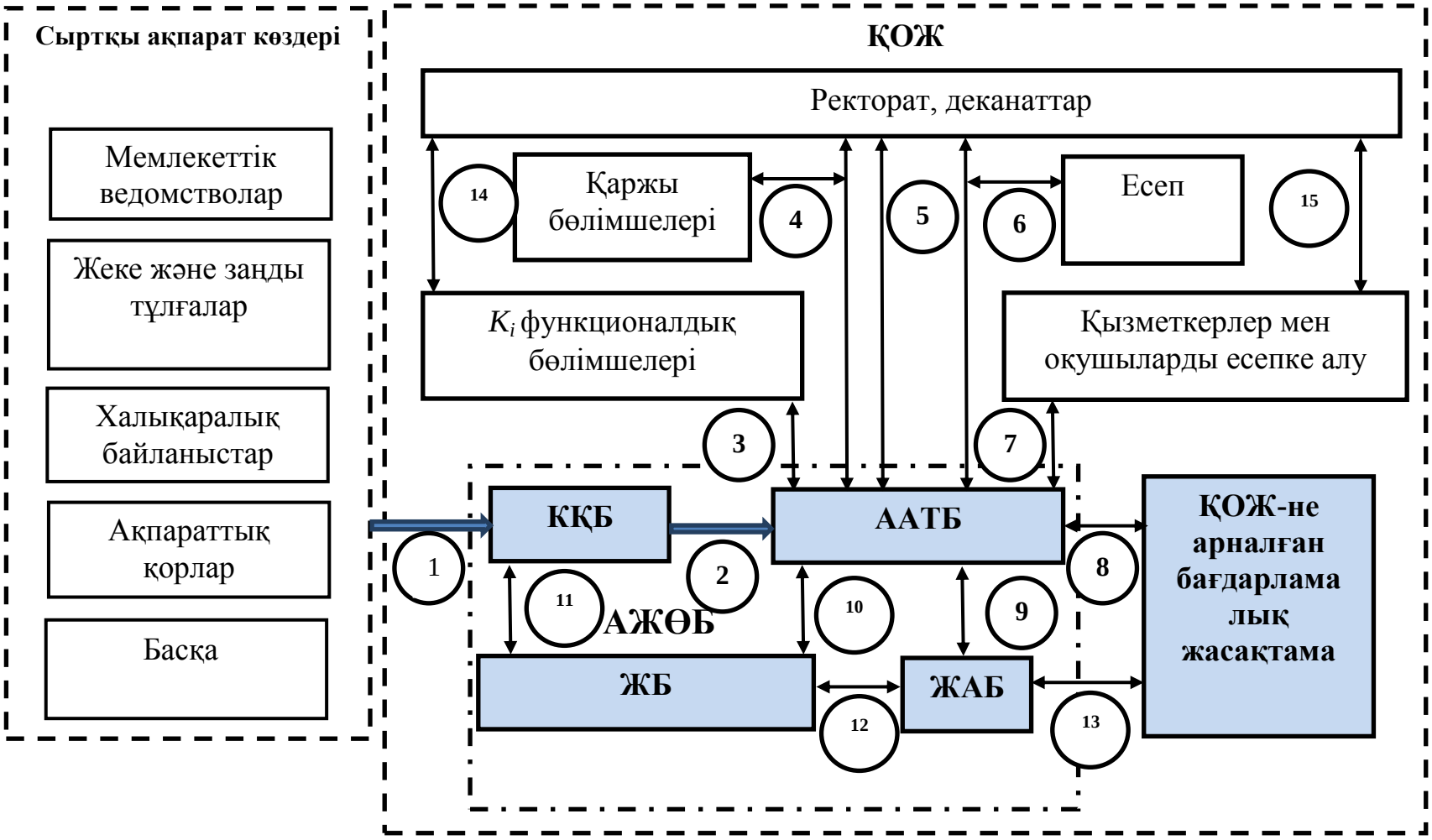
– қашықтықтан оқыту жүйесінің оқытушылары мен білім алушыларының жеке мәліметтерінің құпиялылығын қамтамасыз ету.

Жоғарыда айтылғандарды негізге ала отырып, қашықтықтан оқыту жүйесінің құрылымын және оның негізгі ақпараттық ағындарын тек қана қашықтықтан оқыту жүйесіне қойылатын функционалдық талаптарға сүйеніп қана қоймай, сондай-ақ осындай жүйелердің ақпараттық және киберқауіпсіздігін қамтамасыз ету жөніндегі міндеттерді шешу қажеттілігін назарға ала отырып ұсынуға болады. 3- суретте құрылымдық схема көрсетілген.

Бұл тәсіл қажетті көлемде қашықтықтан оқыту жүйесіне қойылатын негізгі талаптарды ескеруге, сондай-ақ жүйе шеңберінде ақпараттық ағындарды қорғау жөніндегі міндеттерді назарға алуға мүмкіндік береді.

Суретте «1» ретінде белгіленген, сыртқы ақпараттық ағын пайда болған жағдайда, олар қашықтықтан оқыту жүйесіне түспес бұрын алдын ала ақпаратты жинау мен өңдеуге жауап беретін блокта өңделуі тиіс.

Бұл блок [21–27] ұсыныстарына сәйкес келесі функцияларды жүзеге асырады:



Сурет 3 – Киберқауіпсіздікті қамтамасыз ету қажеттілігін ескере отырып, қашықтықтан оқыту жүйесінің ақпараттық ағындарының схемасы

– кіріс трафикті талдау және қашықтықтан оқыту жүйесін сыртқы қатерлерден қорғау (киберқауіпсіздік блогы –КҚБ);

– ақпараттық ағындарды талдау (ақпараттық ағындарды талдау блогы – ААТБ). Бұл блок арналған:

а) ақпараттық ағындардың мониторингі – қашықтықтан оқыту жүйесінің айналымдағы ақпараттық ағындарын бақылау, сондай-ақ олардың есебін жүргізу және статистиканы жинақтау;

ә) ЖОО-ның функционалдық бөлімшелерінен түскен ақпараттық ағындарды талдау;

б) ақпараттық ағынды кодтау-қайта кодтау және тек білім алушыларға арналған арнайы ақпараттық ағынды қалыптастыру;

в) ақпараттық ағынды бағдарлау;

г) ішкі қатерлерден қорғау;

– жоспарлау (жоспарлау блогы–ЖБ). Бұл блок қашықтықтан оқыту жүйесінің айналымдағы ақпараттарды жинау, сақтау және резервтік қайталауға арналған;

– жүзеге асыру (жүзеге асыру блогы–ЖАБ). Бұл блок жоспарлау блогында жинақталған жоспарлар мен деректерді кейіннен имплементациялауға арналған.

Келтірілген функциялардың әрқайсысы қойылған міндеттерді шешу үшін өз алгоритмдері жұмысының негізінде жүзеге асырылуы мүмкін. Барлық блоктардың үйлестірілген жұмысы «потенциальды қатерлі» немесе «зиянды ағындарды» (вирустар, спам және басқалар) ажыратуға қабілетті, бұл қашықтықтан оқыту жүйелері үшін көптеген сыртқы және ішкі киберқатерлерді жүзеге асыруды болдырмауға мүмкіндік береді.

КҚБ-да сәтті тексеру кезінде (Ақпараттық ағын) АА-1 ақпараттық ағыны талдау блогына беріледі, оның блок схемасы 4-суретте көрсетілген.

Жоғарыда көрсетілгендей, ААТБ қашықтықтан оқыту жүйесінде барлық айналымдағы ақпараттық ағындарды бағалау және өңдеу бойынша жұмысты орындайды, ал ең бастысы «кодталған АА» мәртебесін тіркейді және талдауды орындайды. Егер ААТБ-дағы ағымдағы ақпараттық ағын берілген күйден тексеруден өтпесе, оған қатысты кодтау рәсімі орындалады. Кодтау арқылы біз көптеген мақсаттар мен мағыналық элементтер негізінде формалданған құрылымы бар жаңа ақпараттық ағын қалыптасатын процедураның жүзеге асырылуын түсінеміз. Ол төмендегідей өрнекке сәйкес:

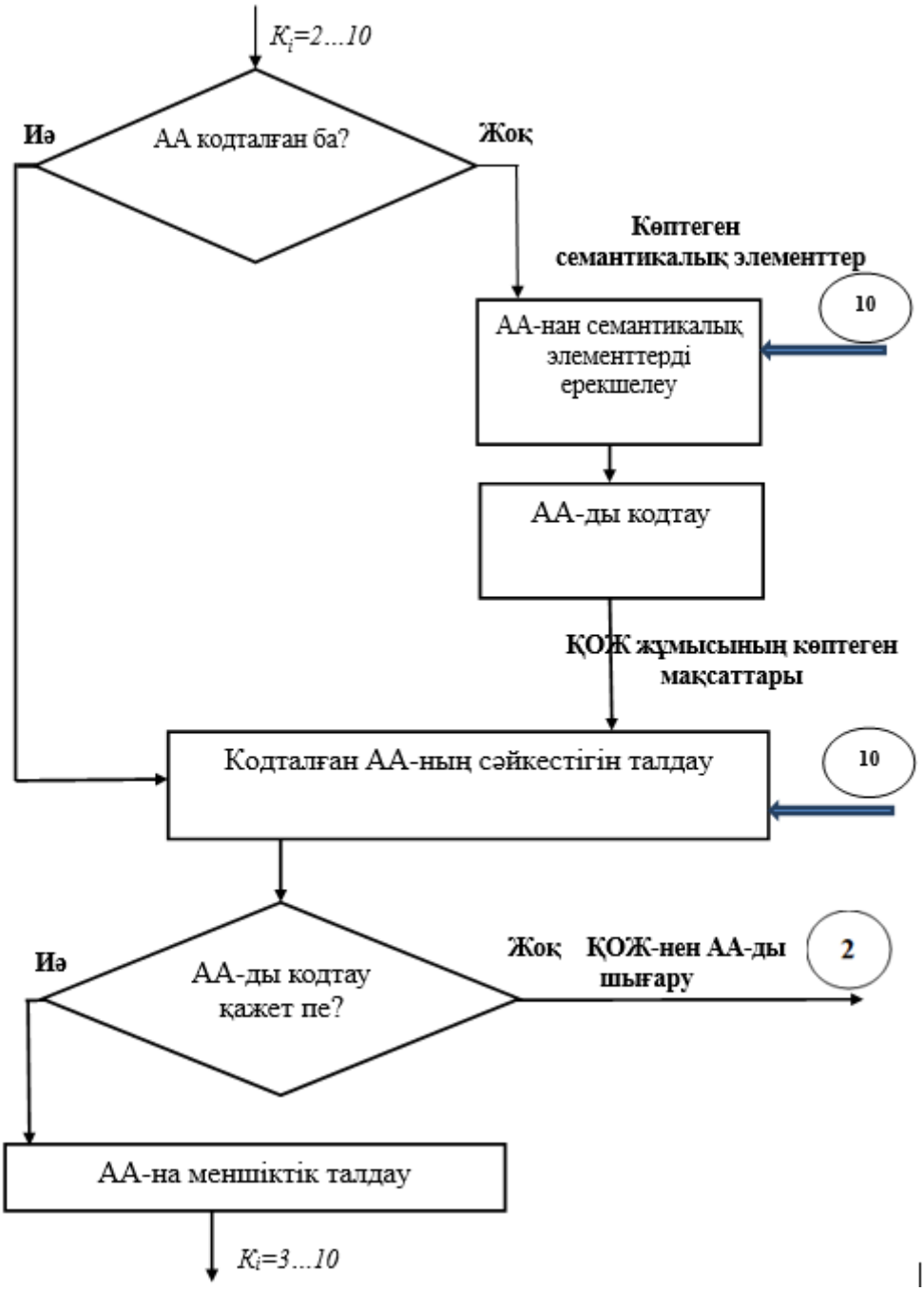
$$M_{C\,INFL} = [M_{ind}, M_{sem}, M_{con}], \tag{1.1}$$

мұнда $M_{C\,INFL}$ – кодталған ақпараттық ағындардың құрылымы;

M_{ind} – ақпараттық ағындардың тиістілігін анықтайтын индекстер жиыны;

M_{sem} – ақпараттық ағындардың мағыналық мазмұнды жиыны;

M_{con} – ақпараттық ағынға сәйкес келетін бастапқы мазмұн жиыны.



Сурет 4 – Талдау блогындағы ақпараттық ағындарды өңдеуге арналған блок схема

Осылайша, «1-2» ақпараттық ағындар аумағында базалық ішкі қатерлерден қорғауды жүзеге асыруға болады. Әрине, бұл үшін қашықтықтан оқыту жүйесінің айқын архитектурасына сүйене отырып, оны қорғаудың адекватты құралдары мен әдістерін таңдау қажет [28].

Мақсатты немесе кездейсоқ зиянды ақпараттық ағындардың қашықтықтан оқыту жүйесінде өңделуі үшін, ол бастапқыда жүйеде қабылданған ақпараттық ағын форматына келтірілуі тиіс. Әйтпесе, бұл ағынды елемейді. Бұл ретте,

кодталғаннан кейін бастапқы ақпараттық ағын өзінің бастапқы белсенділігін жоғалтады, демек, қашықтықтан оқыту жүйесі үшін тікелей қатер төндірмейді.

Егер ақпараттық ағын барлық қойылатын талаптарға, бірінші кезекте ақпараттық қауіпсіздік және киберқауіпсіздік бойынша жауап беретін болса, онда M_{ind} жиын негізінде бұл ақпараттық ағын алгоритмі мен маршрутизация міндеттеріне сүйене отырып, өзінің адресаттарына жіберіледі. Бұл ақпараттық ағындар 4 суретте 3-10 позициясымен белгіленген. Сонымен қатар, қашықтықтан оқыту жүйесі бүгінде әлемнің ЖОО-ның цифрлық ортасында кеңінен қолданылатын электрондық құжат айналымы (ЭҚА) жүйесімен жұмыс істейді деп санаймыз [29–32].

ҚОЖ-де және ЭҚА жүйесіне түсетін айналымдағы ақпараттық ағындарды ұйымдастыру қашықтықтан оқытуды ұйымдастыруға жауапты ЖОО-ның барлық құрылымдық бөлімшелерінің тиімділігін арттыруға мүмкіндік береді, ол ең алдымен өзінің функционалдық мәселелері шеңберінде нақты ақпараттық ағынның өзектілігі есебінен.

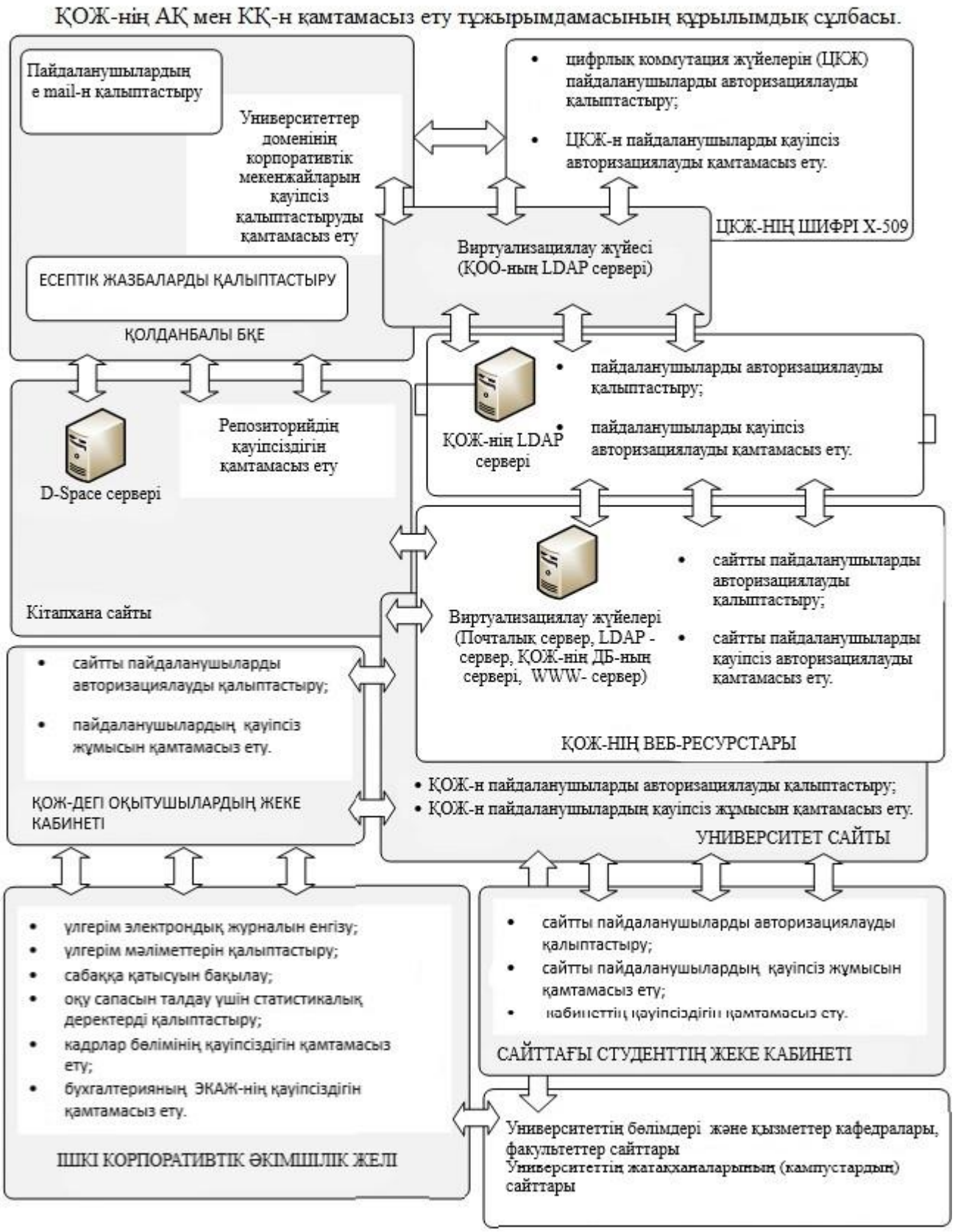
Қашықтықтан оқыту жүйесіндегі ақпараттық массивтердің (АМ) өзектілігін және олардың резервтік көшірмелерін қолдау үшін жоспарлау блогы (ЖБ) пайдаланылады. Бұл ақпараттық массивтерді қалпына келтіру және кездейсоқ іркіліс немесе компьютерлік зиянкестер тарапынан қашықтықтан оқыту жүйесіне мақсатты түрде деструктивті әсер ету жағдайларында олардың тұтастығын бақылау жөніндегі мәселелерді шешуге ықпал етеді.

Талданатын ақпараттық ағын белгілі бір курсты немесе басқа оқу контентін ұсынуға сұраныс болған жағдайда, ақпараттық ағындарды талдау блогына кейіннен жүзеге асырылу блогына түсетін басқару әсерлері автоматты түрде қалыптастырылуы тиіс. Оларды орындау нәтижесі сұранысты жүзеге асыруға ықпал ететін элементтерден тұратын виртуалдық ортаны қалыптастыру болады.

[33–40] жұмыстарында ұсынылған модельдердің синтезі негізінде қашықтықтан оқыту жүйесінің ақпараттық қауіпсіздігі мен киберқауіпсіздігін қамтамасыз ету тұжырымдамасының құрылымдық схемасы және оның ағымдағы жағдайын бағалау ұсынылған (сурет 5).

Бұл тұжырымдама қашықтан оқыту жүйесінің методологиясы [33–40] мен ақпараттық ағындарының схемасын құрудағы белгілі тәсілдермен бірге қашықтықтан оқыту жүйесінің ақпараттық қауіпсіздігін қамтамасыз ету жүйесін құрудың принципті жаңа әдістемесінің негізінде құрылады. Ол келесі кезеңдерді қамтиды:

- ҚОЖ-дегі АҚ және КҚ қатерлерінің әсер ету ықтималдығын анықтау;
- ҚОЖ-дегі АҚ және КҚ деңгейінің жалпыланған көрсеткішін анықтау;
- ҚОЖ-дегі АҚ және КҚ-тегі инвестициялардың тиімділігін бағалау;



Сурет 5 – ҚОЖ-нің АҚ мен КҚ-н қамтамасыз ету тұжырымдамасының құрылымдық сұлбасы

− ҚОЖ-дегі АҚ және КҚ-ті қамтамасыз етудің интеграцияланған алгоритмдерін құру.

Ұсынылып отырған әдістеме, біздің ойымызша, қашықтықтан оқыту жүйесінің айналымдағы ақпараттық ағындарды бақылау мен өңдеудің қазіргі, сондай-ақ жаңа перспективалы механизмдерінің кешенді өзара іс-қимылын тиімді жүзеге асыруға қабілетті. Бұл ретте қашықтықтан оқыту жүйесінің киберқауіпсіздігін инвестициялаудың ұтымды стратегиясымен бірге, сондай-ақ қолданыстағы және перспективалы ақпараттық желілер негізінде қашықтықтан оқытудың функционалды тұрақты және қорғалған жүйесін құрудың модельдерін, әдістері мен ақпараттық технологияларын құру бойынша диссертацияда одан әрі шешілетін ғылыми міндеттерді ескере отырып, жұмыстың 2 тарауында қашықтықтан оқыту жүйелері үшін киберқатерлерді анықтау және алдын алудың әдістері мен модельдерін толықтыру мен дамытудың теориялық аспектілері туралы айтылады [41].

1.3 ЖОО-дағы қашықтықтан оқыту жүйесінің ажырамас элементі ретінде бұлттық технологиялардың киберқауіпсіздігі және функционалды тұрақтылығы

Диссертацияның 1.1 бөлімінде орындалған ғылыми дереккөздерді талдау негізінде оқыту процесінде бұлттық технологияларды қолдану іс жүзінде барлық қызмет салаларында, атап айтқанда, оқу материалына қол жеткізудің тең жағдайларын қамтамасыз ету, субъектілер (оқытушы мен студенттер) арасындағы оқу өзара іс-қимыл және ынтымақтастық есебінен мамандардың құзыреттілігін қалыптастыруға ықпал ететіні анықталды.

Жоғары оқу орындарында ақпараттық технологияларды дамыту деректерді өңдеу орталықтарында (ДӨО) орналасқан бұлттық ресурстарды кеңінен пайдаланумен сипатталады. Мұндай орталықтар - олардың функционалды тұрақтылығы мен киберқауіпсіздігін арттыру мақсатында бір аймақта орналасқан серверлер жиынтығы [42].

Функционалды тұрақтылық киберқауіпсіздік ұғымына қарағанда кең екенін атап өткен жөн. Киберқауіпсіздіктің классикалық түсіндірмесіне сәйкес-бұл функционалды тұрақтылық элементтерінің бірі. Алайда, бұл 1.3 бөлімінде біз ЖОО-ның ҚОЖ-дегі виртуалдық бұлттық сервистердің киберқауіпсіздігі туралы айтамыз, сондықтан төмендегілерді айта кету керек:

− МемСт 33433-2015 сәйкес, қатер-бұл зиян келтірудің потенциальды көзі. Өз кезегінде, киберқауіпсіздік-бұл қашықтықтан оқыту жүйесі үшін қолайсыз тәуекелдің болмауы. Салдарға байланысты жеке қарауға болады: а) ҚОЖ-нің функционалды сенімділігі, егер ол мәселелерді орындауға қатысатын барлық жүйелердің тізбегінде өз функциясын (атап айтқанда, белгілі бір қасиеттерін жоғалтпаса) атқаратын болса; ә) қашықтықтан оқыту жүйесінің функционалды киберқауіпсіздігі, егер оның жұмыс істеуінің бұзылу салдары қолайсыз тәуекелдерге әкеп соқпаса;

− ЖОО-ның ҚОЖ-нің компоненті ретіндегі виртуалдық бұлттық орта тек белгілі қатер класына ғана ұшырайды, демек, шабуылға да. Атап айтқанда,

мысалы, виртуалдық желіні вируспен жұқтырудың мағынасы жоқ, өйткені желідегі виртуалдық машиналар вирусты жұқтырса да, виртуалдық дискілер резервтік көшірмелерден өте тез ауыстырылуы мүмкін;

− киберқауіпсіздік саласындағы мамандардың көптеген жарияланымдарында шабуылдарға және рұқсатсыз қолжетімділікке (РҚЖ) функционалды тұрақты ақпараттық жүйелер ақпараттық қауіпсіздіктің ажырамас бөлігі ретінде қарастырылады. Шын мәнінде, ақпаратты қорғаудың болмауы ақпараттық жүйелерді (атап айтқанда, ҚОЖ) қаскүнемдер тарапынан олардың жұмысына араласудың кез келген деструктивті әрекеттеріне функционалды тұрақсыз етеді.

[43, 44] авторлар бұлттық есептеуді (БЕ) келесідей анықтайды. «Бұл баптауға жататын есептеу ресурстарын қамтитын жалпы пулға желі арқылы барлық жерде және ыңғайлы қол жеткізуді қамтамасыз ету моделі. Мұндай ресурстарға: коммуникациялық желілер, серверлер, деректерді сақтау құралдары, қосымшалар мен сервистерді жатқызуға болады. Ресурстар ең аз пайдалану шығындарымен немесе провайдерге жүгінумен жедел түрде орындалуы мүмкін».

Бұлттық технологияларға кәсіпорынның IT-инфрақұрылымына өз шығындарын оңтайландыруға тырысатын ірі холдингтер де, шағын компаниялар да, немесе өз инфрақұрылымын бірден дамытуға мүмкіндігі жоқ оқу орындары да қызығушылық танытуда. Сондай-ақ, қарапайым пайдаланушылар мүдделі тұлғалар ретінде әрекет етеді. Бұл ретте қарапайым пайдаланушылар ең алдымен деректерді сақтау және бағдарламаларды пайдалану мүмкіндігіне қызығушылық танытады. Бұлттық ресурстарды пайдалану барысында тұтынушылар ДӨО-н құруға, жабдықтардың серверлік және желілік компоненттерін сатып алуға, өз кәсіпорындарының АТ-инфрақұрылымының үздіксіздігін және жұмысқа қабілеттілігін қамтамасыз етуге, күрделі шығындарды айтарлықтай төмендетуге мүдделі. Бұлттық пайдалану кезінде барлық осы ресурстарды қажет ететін және күрделі мәселелер пайдаланушылардан бұлттық қызмет провайдерлеріне беріледі. Пайдаланушы нақты қызметтерді ғана төлейді. Сондай-ақ, бұлттық қызметтері пайдаланушыларға конфигурацияның икемділігін ұсынады. Мысалы, өңдеу қуаттылығы, файлдарды сақтау көлемі, бағдарламалық қамтамасыз ету құрамы (БҚЕ) және т.б. сияқты параметрлерді дербес реттеуге болады.

Бұлттық есептеулердің айқын артықшылықтарына қарамастан, проблемалық мәселелер туындайды. Олардың негізгілері: сервис жеткізушісіне сенімсіздік; бұлттағы ақпараттың құпиялылығын, тұтастығын, түпнұсқалығын сенімді түрде қамтамасыз ету қажеттілігі; ақпараттың барлық кезеңдеріндегі функционалды тұрақтылығы; үздіксіз жұмыс істеуге және рұқсатсыз қолжетімділіктен (РҚЖ) қорғауға кепілдік беру; бұлтқа жіберілетін және өңделетін пайдаланушылардың жеке деректерін сақтау.

Бұлттағы АТ-мен жұмыс істеу кезіндегі құпиялылық - бұл жеткізушілердің мәселесі ғана емес, олар үшінші тұлғалар тарапынан сақталатын деректердің физикалық және бағдарламалық тұтастығын қамтамасыз етуі керек. Қазіргі

заманғы «бұлттық» деректерді өңдеу орталықтары, әдетте, киберқауіпсіздік саласындағы ең заманауи стандарттарға сүйене отырып (антивирустық қорғау, шифрлау, кіруді анықтау жүйелері (КАЖ) және т.б. мәселелерін қоса алғанда) негізделеді.

Деректерді өңдеу орталығындағы серверлердің функционалды тұрақтылығы желілік және физикалық қорғаныспен, сондай-ақ ақауларға төзімділікпен және сенімді қуат көзімен қамтамасыз ету құралдарымен қамтамасыз етіледі. Бүгінгі күні нарықта мәселелердің тар шеңберіне бағдарланған серверлердің функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету үшін аппараттық-бағдарламалық шешімдердің кең спектрі ұсынылған. Алайда, классикалық аппараттық және бағдарламалық жүйелерді виртуалдық платформаларға біртіндеп ауыстыру салдарынан, мұндай мәселелердің саны айтарлықтай артты және өсіп келеді.

Функционалды тұрақтылығы мен киберқауіпсіздігі тұтастығы үшін қатерлердің белгілі түрлеріне (желілік шабуылдар, операциялық жүйелер (ОЖ) қосымшаларындағы осалдықтар, зиянкес бағдарламалық қамтамасыз етулер) соңғы жылдары жаңалары қосылды. Мұндай жаңа қатерлерге ортаны бақылауды ұйымдастыру (гипервизор), қонақ машиналары арасындағы трафикті бақылау және қол жеткізу құқығын шектеудегі қиындықтар жатқызуға болады. Сондықтан қазіргі заманғы деректерді өңдеу орталықтарының бірқатар салаларда жұмыс жасауы – олардың функционалды тұрақтылығын қамтамасыз ету үшін техникалық талаптардың деңгейін жоғарылатуды талап етеді. Бұл білім берудегі бұлттық технологияларға ғана емес, сонымен қатар, аса маңызды бұлттық архитектураға да толық қатысты мысалы, банктерде, көлік өнеркәсібінде, критикалық маңызды компьютерлік жүйелердің инфрақұрылымында қолданылуы мүмкін.

Виртуалдандыру технологияларының пайда болуы және дамуы көптеген жүйелердің виртуалдық машиналарға (ВМ) кең ауқымда көшуіне әкеп соқтырды. Бұл ретте жаңа ортада бағдарламалық қамтамасыз етуді пайдалануға қатысты функционалды тұрақтылығы пен киберқауіпсіздігін қамтамасыз ету мәселелерін шешу өзгеше тәсілді талап етеді. Киберқатерлердің көптеген түрлері жеткілікті зерттелген және олар үшін сәйкес қарсы тұру құралдары мен әдістері әзірленді. Алайда мұндай әдістерді бұлтта пайдалану үшін бейімдеу қажет. Виртуалдандыру технологияларына негізделген платформалардың енуі - бұл жүйелерді пайдаланатын барлық компаниялар бұлттың функционалды тұрақтылығы мен киберқауіпсіздігі мәселелерімен белсенді айналыса бастады.

Қазіргі уақытта виртуалдық бұлттық ресурстарының функционалды тұрақтылығы мен киберқауіпсіздігін арттыру бойынша көптеген мәселелер толық зерттелмеген [43,44]. Қолданыстағы әзірлемелерде [45, 46] проблеманың осы түрін шешудің маңызды кемшіліктері бар [47]. Атап айтқанда, бірқатар зерттеушілер [48, 49] бұлттық ресурстарының функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету үшін универсальды әдістің болмауына байланысты екенін көрсетті:

− бұлттық ақпараттық жүйелердегі қолданыстағы виртуалдық машиналардың мүмкіндіктерінің үнемі өзгеруі;

− қорғалмаған қосымшалар интерфейстерін пайдалану;

− қолданыстағы жүйелердің жоғары қарқындылығы.

Бағдарламалық-конфигурацияланатын желілер - бұл деректерді жіберудің виртуалдық желілерінің бір түрі, онда желілерді басқару деңгейі деректерді жіберудің физикалық құрылғыларынан бөлінген, ал басқару бағдарламамен жүзеге асырылады. Бағдарламалық-конфигурацияланатын желілер негізінде виртуалдық бұлттық ресурстардың (ВБР) функционалды тұрақтылығын қамтамасыз етудің қазіргі заманғы әдістері [43-49] жұмыстарымен тығыз байланысты.

[50,51] жұмыста бағдарламалық-конфигурацияланатын желілер негізіндегі ВБР-ның функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету мәселесін шешудің маңыздылығы мен өзектілігі негізделген. Алайда, бұл жұмыстарда негізінен шолу жүргізілген.

[52,53] жұмыстарда авторлар бұлттық технологиялардың тиімділігіне талдау жүргізді, соның негізінде оларды қолдану дәстүрлі технологиялардың ақпараттық технологияларының алдында бірқатар артықшылықтары бар деген қорытынды жасалды. [54] жұмыста ұйымның есептеу ресурстарын тиімді басқару мәселелеріндегі виртуалдық бұлттық ортаның (ВБО) артықшылықтары көрсетілген. [43-49] виртуалдық бұлттық ортаның артықшылықтары АТ-инфрақұрылымға және ақпараттандыру нысанының қызмет көрсету персоналына қызмет көрсетудің құнын төмендету, деректерді шығын мен шабуылдардан сенімді қорғауды қамтамасыз ету мәселелеріне негізделген. Алайда, бұл жұмыстарда виртуалдық бұлттық орталарының функционалды тұрақтылығын арттыруға бағытталған нақты әдістемелердің сипаттамасы болған жоқ. [45, p.215-222, 46, p.252-263] жұмыстарында оқу іс-әрекетінің көптеген түрлерін орындау, бақылау және бағалау, онлайн тестілеу үшін виртуалдық бұлттық орталарын қолданудың практикалық аспектілері қарастырылған. Бұл ретте білім беру ұйымдарындағы виртуалдық бұлттық ортаның киберқауіпсіздігіне қатысты мәселелер қарастырылған жоқ.

[47, p.285, 48, p.97] жұмыстарда виртуалдық бұлттық орталарының функционалды тұрақтылығына күрделі басқару нысандарының сенімділік қасиеттерін жоғарылату мәселелерін шешудің жүйелік тәсілдерінің негізінде қол жеткізілетіні көрсетілген. Сонымен қатар, [44, p.5, 48, p.98] айтылғандай, функционалды тұрақтылық-бұл сенімділік пен тұрақтылықтан принципті ерекшеленетін сипат. Функционалды тұрақтылығын қамтамасыз ету әдістері күрделі техникалық жүйелердің қолданыстағы техникалық ресурстарын неғұрлым толық пайдалануға бағытталған. Виртуалдық бұлттық ортасының функционалды тұрақтылық пен киберқауіпсіздікті қамтамасыз ету мәселесі қазіргі басқару теориясының өзекті ғылыми міндеттерінің бірі ретінде қарастыруға болады [49, p.1020].

Талданған ғылыми зерттеулер бұлттық пайдаланушылар үшін ең маңызды факторлар функционалды тұрақтылығы мен қауіпсіздігі маңызды болып

табылатындығын көрсетті. Бұлттық виртуалдық ресурстардың ішкі тұтастығын бұзу үшін виртуалдық бұлттық орталарына хакерлердің сыртқы әсері [44, p.10 50, p.145] жұмыстарында функционалды тұрақтылығына қатер ретінде қарастырылады. Бұл ретте мұндай әсер жүйеге кіру үшін бұлттық пен оның ресурстарындағы осалдықтарды пайдалана алады. Жүйелік администраторлар хост-машинаны толық басқаратын дәстүрлі ДӨО-да мұндай сыртқы әсерлер орталықтандырылған түрде анықталады және түзетіледі. Алайда, бұлттық пайдаланушылар өздерінің виртуалдық машиналарына бағдарламалрды басқаруға артықшылықтары бар деректерді өңдеу орталықтарындағы функционалды тұрақтылығы мен киберқауіпсіздік шаралары тиімді жұмыс істей алмайды. Бұл, өз кезегінде, «қызмет көрсету деңгейі туралы келісім» талаптарының бұзылуына әкеледі. Сонымен қатар, пайдаланушылар осал бағдарламалық жасақтаманы бұлттағы виртуалдық машиналарға орната алады. Бұл бұлттық ортаның функционалды тұрақтылығын айтарлықтай төмендетеді. Осылайша, сыртқы әсерлерге, оның ішінде хакерлер мен басқа да қаскүнемдерден деструктивті әрекеттерін анықтауға және оларға жауап қайтарудың тиімді жүйесін құру мәселесі релеванттық болып қала береді. Бұл бұлттық виртуалдық ресурстардың функционалды тұрақтылығын бұзу салдарын барынша азайту үшін уақытылы ақпарат алу үшін қажет.

Жүргізілген талдау шабуыл граф түрінде виртуалдық бұлттық ресурстарға шабуыл жасау модельдерін құру бағытында зерттеулерді жалғастыру қажет екенін көрсетті. Бұл шабуылдаушының әрекетін сипаттауға және болжауға мүмкіндік береді.

1.4 ЖОО-ның қашықтықтан оқыту жүйелерінің киберқауіпсіздігіне инвестициялау стратегияларының математикалық модельдерін талдау

Қазіргі уақытта, ақпарат кез келген компания немесе оқу орны үшін ең құнды актив болып табылады. Ақпарат және ақпараттық технологиялар (АТ) оқу орындарындағы барлық бизнес-процестердің негізі болды. Қазіргі заманғы жоғары оқу орындары бүгінгі таңда адами қызметтің барлық салаларындағы инновациялық әзірлемелер мен жобалардың алдыңғы жағында. Жоғарыда атап өткендей, қоғамды жаһандық цифрландыру жағдайында, білім беру саласында қашықтықтан оқыту жүйесін қолдану тек оларға тән сапалық сипаттамалар мен ерекшеліктер есебінен кең таралуда [55].

Жоғары оқу орындарының қашықтықтан оқыту жүйесінің дамуымен параллелді олардың жұмысына деструктивті араласу саны артты. Жоғары оқу орындарының бәсекеге қабілеттілігі мен табысты дамуының негізгі шарты - оның барлық ақпараттық жүйелерінің, оның ішінде қашықтықтан жүйелердің ақпараттарын сауатты түрде қорғау болуы мүмкін екені түсінікті. Сондықтан ЖОО-ның ҚОЖ-нің ақпараттық қауіпсіздігі (АҚ) мен киберқауіпсіздігін (КҚ) қамтамасыз ету жөніндегі мәселелер өзектілендірілді. Көптеген зерттеушілердің пікірі бойынша [56-58], қашықтықтан оқыту жүйесінің ақпараттық қауіпсіздігі мен киберқауіпсіздігі бойынша қолданыстағы типтік шешімдер жоғары оқу орындарының қашықтықтан оқыту жүйелерінің

ақпараттық қауіпсіздігі мен киберқауіпсіздігіне байланысты міндеттерді ішінара ғана шешуге қабілетті.

Жоғары оқу орындарының ақпараттық жүйелеріне заманауи кибершабуылдар, атап айтқанда, олардың қашықтықтан оқыту жүйелеріне, ақпаратты қорғау және киберқауіпсіздік үшін шешімдер қабылдауды қолдау саласындағы есептеулерді интеллектуалдылыққа байланысты зерттеулерді дамыту бойынша ынталандыруға қызмет етті.

Инновациялық жобаларға инвестициялар, мысалы, АТ және КБ саласында, көптеген жағдайларда есептеулердің дәлсіздігінің үлкен ықтималдығымен анықталады. Соңғы жылдары әртүрлі компаниялар жасаған АТ және КБ инвестициялау міндеттерінде шешім қабылдауды қолдау жүйелері (ШҚҚЖ) жақсы пікірге ие болды. ШҚҚЖ-нің кейбірі маңызды ақпараттық жүйелердің киберқауіпсіздігі саласындағы жобаларды қаржылық инвестициялау үшін көп нұсқалы стратегияларды іздестірумен байланысты рәсімдерді оңтайландыруға мүмкіндік береді [56].

Тәжірибелік қолданудағы ең кең таралған модельді 2002 жылы Мэриленд университетінің американдық зерттеушілері Лоуренс Гордон және Мартин Лоеб ұсынған [57]. Жұмыс берілген ақпарат жиынтығын қорғау үшін инвестициялардың оңтайлы сомасын анықтайтын экономикалық модельді сипаттайды. Модель қауіпсіздікті бұзу және осындай бұзу жағдайында потенциалды жою үшін ақпараттың осалдығын ескереді. Осы потенциалды шығын үшін компания өз инвестицияларын ең жоғары осалдығы бар ақпараттық жиынтықтарға міндетті түрде шоғырландырмауы тиіс екендігі көрсетілген. Өте осал ақпарат жиынтықтарын қорғау үшін тым қымбат болуы мүмкін болғандықтан, компаниялар өз күш - жігерін орта деңгейдегі осалдықтардың ақпараттық жиынтықтарына көңіл бөлгені дұрыс. Сондай-ақ талдау ақпаратты қорғау үшін инвестициялардан күтілетін пайданы барынша арттыру үшін фирма қауіпсіздікті бұзудан күтілетін шығындардың аз бөлігін ғана жұмсауы тиіс деп болжайды.

Модель құрылымы статикалық – шешімдер мен нәтиже бір мезгілде басталады, ал динамикалық әсерлер, соның ішінде ақшаның уақытқа тәуелділігі есепке алынбайды. Ақпараттық жинақ клиенттердің тізімі, кредиторлық берешектің бухгалтерлік кітабы сияқты түрлі нысандарын қабылдауға болады,

λ – ақпараттық жиынтықтың қауіпсіздігін бұзудан туындаған ақшалай шығын;

t – шабуыл ықтималдығы, $t \in [0,1]$;

ν – инвестициялар болмаған жағдайда шабуылдар табысты болуы ықтималдығын түсінетін ақпараттың осалдығы λ; $0 \le \nu \le 1$;

z – ақпаратты қорғау шығындары.

$\lambda = const$ моделі үшін, алайда практика жүзінде $\lambda = \lambda(t)$. t шамасы жалғыз шабуылға жатады (бір мезгілде бірнеше шабуылдардың басталуы қарастырылмайды).

Сондай-ақ басқа шамаларды да қарастырады:

νt – шабуыл нәтижесінде шығындар ықтималдығы;

$L = t\lambda$ –ақпараттық активтерге байланысты ықтимал шығындар;

$S(z,\nu)$ – қауіпсіздікті бұзу ықтималдығы.

Ақпараттық осалдықтың және ақпараттық қауіпсіздіктің негізі $S(z,\nu)$ қатысты мынадай болжамдарды (Б1, Б2, Б3) қарауға әкеледі:

Б1. $S(z,0) = 0$ барлығы үшін z. Атап айтқанда, егер ақпарат жинау толығымен қолайсыз болса, ол нөлдік инвестицияларды қоса алғанда, қауіпсіздікке салынатын инвестициялардың кез келген көлемі үшін мінсіз қорғалған болып қалады.

Б2. ν барлығы үшін, $S(0,\nu) = \nu$. Атап айтқанда, егер ақпараттық қауіпсіздікке инвестициялар болмаса, қатерді іске асыруға байланысты қауіпсіздікті бұзу ықтималдығы өзгеріссіз қалады.

Б3. $\nu \in (0,1)$ барлығы үшін және z, $S_z(z,\nu) < 0$ және $S_{zz}(z,\nu) > 0$ барлықтарына, мұнда S_z - z және S_{zz} бойынша жеке туындыны білдіреді S_z-тен z-ке қатысты жеке туындыны білдіреді.

Осылайша, ақпараттық қауіпсіздікке инвестициялардың ұлғаюына қарай ақпарат неғұрлым қорғалған болады. Сонымен қатар, $\nu \in (0,1)$, $\lim S(z,\nu) \to 0$ барлығы үшін, $z \to \infty$ сияқты, сондықтан қауіпсіздікке айтарлықтай қаражат салып, қауіпсіздікті бұзу ықтималдығы t рет $S(z,\nu)$, атап айтқанда нөлге жақындауы мүмкін деген болжам бар[58].

EBIS (Expected Benefits of an Investment in Information Security) ретінде белгіленетін ақпараттық қауіпсіздікке инвестициялардан күтілетін пайда қосымша қауіпсіздікке байланысты фирманың күтілетін шығындарын қысқартуға тең:

$$EBIS(z) = [\nu - S(z,\nu)]L. \qquad (1.2)$$

ENBIS (Expected Net Benefits from an Investment in Information Security) ақпараттық қауіпсіздігіне инвестицияларды салудан күтілетін таза пайда EBIS және инвестициялар құнының әртүрлілігіне тең:

$$ENBIS(z) = [\nu - S(z,\nu)]L - z. \qquad (1.3)$$

Инвестицияның оңтайлы мөлшері деп $z^*(\nu)$ есептейді, онда $ENBIS(z)$ ең жоғары мәнге жетеді.

Б1–Б3 шарттарына жауап беретін осалдықтың функциясының екі класы ұсынылған.

Көрсеткіш функцияларының бірінші класы:

$$S^I(z,\nu) = \frac{\nu}{(\alpha z + 1)^\beta}, \qquad (1.4)$$

$\alpha > 0$, $\beta \geq 1$ параметрлері ақпараттық қауіпсіздік өнімділігінің шаралары (ν және z берілген кезде қауіпсіздікті бұзу ықтималдығы α үшін де, β үшін де азаяды).

$ENBIS_z'(z^*) = 0$ шарттан инвестицияның оңтайлы мөлшерін осылай есептеуге болады:

$$z^{I*}(\nu)=\frac{(\nu\beta\alpha L)^{\frac{1}{\beta+1}}}{\alpha}. \qquad (1.5)$$

Атап айтқанда, (1.5) –ден келесі алынады, бұл

$z^{I*}(\nu)=0$ үшін $0\le\nu\le 1/\alpha\beta L$.

Осылайша, ν шамасы $\nu=\frac{1}{\alpha\beta L}$ - ге дейін ұлғайғанға дейін бірінші класс үшін қауіпсіздікке оңтайлы инвестициялар нөлге тең. ν - қатерлерді жүзеге асыру ықтималдығы одан әрі ұлғайған кезде $z^{I*}(\nu)$ шама (1.4) сәйкес есептеледі.

Көрсеткіш функцияларының екінші класы:

$$S^{II}(z,\nu)=\nu^{\alpha z+1}, \qquad (1.6)$$

мұнда параметр $\alpha>0$ – ақпараттық қауіпсіздік өнімділігінің өлшемі.

$ENBIS_z^{'}(z^*)=0$ шартынан аламыз:

$$z^{II*}(\nu)=\frac{\ln\left(\frac{1}{-\alpha\nu L(\ln\nu)}\right)}{\alpha\ln\nu}. \qquad (1.7)$$

(1.7) шартында $S(z,\nu)$-ші функцияның II класы үшін z^{II*} функциясы алдымен өседі, содан кейін ν ұлғаюымен азаяды.

Гордон-Лоеб моделі жарияланғаннан кейін ғылыми ортада мойындалғанына және оны басқа авторлармен [59-61] және Лоуренс Гордон мен Мартин Лоебтің өздері [62] толықтырғанына қарамастан, көптеген мәселелер әлі де шешілуі керек. Модель авторлары проблеманы алғаш рет негізді түрде қарап, ақпараттық қауіпсіздіктің негізгі көрсеткіші болып табылатын осалдықтың функциясын анықтады.

Модельдің төмендегідей кемшіліктерін анықтауға болады:

− ақша түсімдерінің тұрақты өсу қарқынына байланысты, модель бір фазалы, сондықтан оны ақша түсімдері айтарлықтай өзгеруі мүмкін компанияларды бағалау үшін қолдануға болмайды. Мұндай компаниялар үшін көпфазалы модельді пайдаланған дұрыс. Жоғарыда айтылғандарға сүйене отырып, біз бұл модель - өсу үшін барлық мүмкіндіктері таусылған үлкен компанияларды бағалау үшін неғұрлым қолайлы деген қорытынды жасауға болады;

− кіріс ақпаратына тым сезімтал, дивидендтік саясаттың өзгеруін, акцияларды кері сатып алуды және басқаларды назарға алмайды;

− негізінен, тәуекелдерді басқарудың оңтайландыру аспектілерін зерттеуге есептелінеді, бұл нақты тәуекел нысанын есепке алу мүмкіндігін барынша азайтады;

− дисконттық мөлшерлеме дивидендтер төлемдерінің өсуіне қарағанда жоғары.

Вухен Шим Гордон-Лоеба жұмысына негізделе отырып, екі бірдей кәсіпорын үшін өзара байланысты тәуекелдердің моделін жасады[63]. Автор

теріс сыртқы әсерлер кезінде киберқауіпсіздіктегі салымдардың оңтайлы саны тәуелсіз тәуекелдер кезінде салымдардың оңтайлы санына тең немесе артық болатынын, ал нөлдік салымдар аймағы аз болатынын көрсетті. Егер кәсіпорындардың ынтымақтастығы оң сыртқы әсерлер туғызса, онда киберқауіпсіздіктегі салымдардың оңтайлы саны тәуелсіз тәуекелдер кезінде салымдардың оңтайлы санына көбірек немесе тең болады,ал нөлдік салымдар аймағы тәуелсіз тәуекелдермен бірдей үлгі болады.

Бұдан басқа, Шим [64] мақсатты емес шабуылға қарсы тұруға бағытталған және сезімтал жүйелердің мүмкін болатын санына зиян келтіруге бағытталған қаржылық инвестициялар оң сыртқы әсерлер тудыратынын теориялық және эмпирикалық түрде дәлелдеді, өйткені ұйымның қаржылық салымдарының ұлғаюы осы фирманың жүйесімен қосылған басқа компаниялардың тәуекелдерін төмендетеді. Нәтижесінде 6-суретте көрсетілгендей, сыртқы әсерлердің проблемалары мен шабуыл түрлері арасындағы өзара байланыс бейнеленген.

Жоғарыда аталған екі модельдің де кемшіліктері бар. Олардың ешқайсысы динамикалық режимде оңтайлы шешімнің есебін, атап айтқанда қаржылық салымдардың әсерін ескермейді. Мысалы, құқық бұзушы киберқауіпсіздікке қосалқы қаржы салымдары пайда болғаннан кейін өз шабуылдарының стратегиясын қалай өзгертетінін талдамайды. Осы модельдердің әрқайсысы үшін шығындарды сандық бағалау, қатердің туындау ықтималдығын бағалау және жүйенің құқық бұзушылар шабуылына бейімділігін бағалау сияқты деректерді алудың күрделілігі бар. Өзара байланысты тәуекелдер моделі бірдей кәсіпорындар үшін ғана жарамды, сондықтан барлық ұйымдармен жұмыс істеуге жарамсыз. Екі модель де ақпараттық жүйенің осалдығы функциясының екі класына негізделген.

Сурет 6 – Сыртқы әсерлер мен шабуыл түрлері арасындағы байланыс

В.К. Задирака және бірлескен авторлардың [65] жұмысында ақпаратты қорғауға арналған шығындар мөлшерін анықтау үшін модельдің нұсқасын қарастырады, ол ұйымдарға ақпарат қауіпсіздігінің өзіндік жүйесін құру немесе жетілдіру үшін пайдалы болуы мүмкін.

Ақпарат қауіпсіздігіне жұмсалатын шығындардың жалпы күтілетін мөлшерін V шығындар сомасы S және ықтимал шығындар $b(S)$ ретінде көрсетуге болады:

$$V = S + b(S). \tag{1.8}$$

(1.8) функциясын min керек, ол мақсат ретінде ұсынылуы мүмкін

$$V(S) = S + b(S) \to \min. \tag{1.9}$$

S ақпаратты қорғауға арналған шығыстарды қаржыландыру $b(S)$ қауіпсіздікті бұзудан күтілетін шығындардың мөлшерін азайтуы тиіс, және де S үлкен мәндеріне $b(S)$ аз мәндерге жауап беруі тиіс:

$$0 < S_1 < S_2 \Rightarrow b(S_2) < b(S_1) < b(0) = B. \tag{1.10}$$

(1.10) формуласы $b(S)$ функциясы монотонды төмендейтінін білдіреді, сондықтан тұтыну көлеміндегі күтілетін шығындардың $b(S)$ өзгеру жылдамдығы теріс:

$$b'(S) < 0. \tag{1.11}$$

S – шығындардың максималды мәні келесі түрде алынады:

$$S_{\max} = \frac{\nu B^{1-\nu} - B^{1-\nu}}{(\nu - 1)(\nu B^{1-\nu})\frac{\nu}{\nu - 1}} = \frac{(B^{1-\nu})^{\frac{1}{\nu-1}}}{\nu \frac{\nu}{\nu - 1}} = \frac{B}{\nu^{\frac{\nu}{\nu-1}}}. \tag{1.12}$$

Глушак-Новиков [66, 67] жұмысында зиянкестің шабуылдарының кешенді сипаты және қорғау жүйесін құруға қорғаушы ресурстарының шектеулілігі шартымен ақпаратты қорғау жүйесін құру бойынша есептерін шешу әдісі ұсынылған. Әзірленген модель бойынша зиянкестер және жүйеде бар осалдықтар туралы ақпарат болған кезде қорғау жүйесін құруға арналған шығындардың кемуі бойынша оңтайландыру есебі қалыптасты.

Зерттеу нысаны ашық архитектурасы бар үлестірілген ақпараттық-коммуникациялық жүйе (АКЖ), ол ақпаратты өңдеуге қатысатын C өзара әрекет ететін компоненттерден тұрады. Әрбір компонент сипаттамалар жиынтығымен сипатталады, олардың арасында ақпаратты өңдеу технологиясы, операциялық орта және т.б. жатады. Компоненттердің көрсетілген параметрлері q_c-ден кейін белгіленетін жүйе үшін олардың құндылығын құрайды.

Есептеу ортасының сипаттамаларын ескере отырып , компоненттердің әрқайсысы A мүмкін болатын қатерлерден белгілі бір қатерлерге осал болып табылады. Ақпараттық коммуникациялық жүйенің архитектурасы туралы ақпарат қақтығыс тараптарына ашық және белгілі деп есептейді. Сонымен қатар, c жүйе құрауышына қарсы α-ші қатердің сәтті жүзеге асырылу ықтималдығы, сондай-ақ p қорғау механизмдерін орнатумен қатерді бейтараптандыру ықтималдығы берілген. Осылайша, қаскүнем немесе қорғаушы қабылдаған шешімдердің тиімділігіне кездейсоқ факторлар әсер етеді, оны модельдеу кезінде ескеру қажет.

Қорғаушы мен қаскүнем арасындағы қарым- қатынас тәуекел функциясын пайдалану арқылы қалыптастырылуы мүмкін. Қаскүнем жүйеге зиян келтіре отырып, тәуекелді барынша арттыруға тырысады. Сонымен қатар, қорғаушы, зиянкеске қарсы әрекет ету, нөлге қатерлерді азайтуға ұмтыла отырып, қорғау механизмдерін орнатады. Қаскүнемдің берілген моделі бойынша қаржылық және техникалық ресурстардың шектеулілігі жағдайында қорғаушы ақпараттық коммуникациялық желілердегі тәуекел барынша аз болатындай етіп құралдар мен қорғау шараларын бөлу қажет. Ойын теориясының терминдерінде тәуекел функциясы төлем функциясы болып табылады. Тәуекелдерді бағалау үшін сандық шама Q_c келтірілген шығын, бұл шығындар мен алынбай қалған пайда түрінде көрсетіледі. Осылайша, Q_c залалдың мәні жүйенің жалпы жұмыс істеуі үшін осы q_c компонентінің құндылығына баламалы C белгілі бір компоненттен туындады. Жалпы түрде ақпараттық қауіпсіздік тәуекелінің R_{ac} функциясы үшін арақатынасты α-ші қатерді жүзеге асыру $P_{ac}^{\sim}$ ықтималдығының туындысы және осы қатерді жүзеге асыру кезінде келтірілген зиян Q_c ретінде жазуға болады. V_{ac} айнымалысы белгіленген қосымша қорғау механизмдерін пайдалана отырып, қатерлерді бейтараптандыру ықтималдығын сипаттайды [66, p.95]:

$$R_{ac} = P_{ac}^{\sim} * Q_c * (1 - V_{ac}). \qquad (1.13)$$

Қорғаушы мен қаскүнем арасындағы қарсы тұру ерекшеліктерінің бірі динамикалық сипат, өйткені шабуыл әдетте модельде ескерілуі қажет жүйені және барлауды бақылау алдында болады. Осылайша, қақтығыс жағдайы уақыт өте келе өзгеруі мүмкін.

Әзірленген тәсілге сәйкес [67, p.50] ақпаратты қорғау жүйесін (АҚЖ) құрылымы келесі кезеңдерге бөлуге болады:

− сараптамалық бағалау әдістерін пайдалана отырып, бастапқы ақпаратты жинау және талдау – құрылымды талдау, осалдықтарды талдау, қатерлерді талдау;

− ақпаратты қорғау жүйесінің құрылымын синтездеу - бірінші кезеңде алынған бастапқы деректерді модельге алмастырамыз. Алынған есепті симплекс әдісін пайдалана отырып шешу нәтижесінде R тәуекелінің салыстырмалы мәні, сондай-ақ қарсы тұру кезінде оңтайлы болатын қорғаныс механизмдерінің жиынтығы алынды.

Rand фирмасының шеңберінде әзірленген екі тараптың қарама қайшылық моделі - тактикалық әскери операцияларды имитациялауға арналған Гросс моделі. Осы модельге сәйкес, қақтығыс тараптар X және Y ресурстарға ие, ал олардың қарама - қайшылық нәтижесі мақсатты функциямен анықталады, ол инвестицияланған ресурстардың айырмашылығына тікелей байланысты және сызықтық бағдарламалау мәселесіне әкеледі:

$$i(x, y) = \sum_{k=1}^{l} i_k(x_k y_k) = \sum_{k=1}^{l} g_k \max(x_k - y_k, 0), \qquad (1.14)$$

мұнда k – нысанының нөмері;

x_k және y_k – k-ші нысандағы шабуыл жасау және қорғау ресурстары;

g_k – салмақ коэффициенті, ол нысандардың маңыздылығын немесе осалдығын көрсетеді.

Мәні $x_k - y_k$ және 0 екі саннан көп болып табылатын $\max(x_k - y_k, 0)$-шама қорғаныс арқылы нысанға дейін енуге қабілетті x_k бөлімшенің бөлігін білдіреді.

Осылайша, $g_k \max(x_k - y_k, 0)$ шамасы k-ші нысанға шабуылдың сәттілігін сандық түрде сипаттайды. Ақпараттық қауіпсіздік мәселелеріне қолданғанда g_k – k-ші нысандағы ақпараттың салыстырмалы құндылығын, ал $g_k \max(x_k - y_k, 0)$-ақпараттың таралып кетуінен келтірілген залалды білдіреді. Келтірілген зиян оның құнынан үлкен болмайтындықтан, $x - y \geq 1$ кезінде $i(x, y) = 1$ қою керек.

Демек, $i(x, y)$ функциясы бөлікті-сызықты сипатқа ие. x айнымалының барлық интервалы y өзгермеген мәнде x_1 және x_2 шектік мәндерімен шектеулі үш аймаққа бөлуге болады

$x < x_1$-де $i(x, y) = 0$ аламыз,

$x > x_1 - i(x, y) = 1$ -де,

$x_1 < x < x_2$-де $i(x, y)$ функциясы g бұрыштық коэффициентімен тікелей өсуде.

Жоғарыда келтірілген пікірлерді ескере отырып, ақпараттың таралып кетуінен келтірілген зиянкесті көрсететін мақсатты функция келесідей түрде алынады [68]:

$$i(x, y) = \sum_{k=1}^{l} g_k (x_k - y_k), \qquad (1.15)$$

где $x_k - y_k = \begin{cases} 0 \text{ при } x_k - y_k \leq 0; \\ \mathrm{x_k} - y_k \text{ при } 0 < x_k - y_k \leq 1; \\ 1 \text{ при } x_k - y_k > 1. \end{cases}$.

Әскери операцияларды жоспарлау кезінде туындаған Гросстың есебі қарастырылған міселелерден бірқатар айырмашылықтарға ие. Біріншіден, мақсатты функция дискретті сипатқа ие, өйткені қорғаныс арқылы кірген немесе шабуыл немесе қорғанысы жойылған бірліктердің санын анықтайды. Екіншіден, бұл бірліктер қарсы тұрудың әрбір кездейсоқ жағдайында шабуыл үшін және тиісінше қорғаныс үшін бірдей. Нысандардың біртиптілігі есепті шешуді айтарлықтай жеңілдетеді, алайда қарсы тұру шарттарын шектейді. Алайда, Гросс моделінің негізгі кемшілігі - оның мақсатты функциясының бөлікті - сызықтық сипаты, ол, әрине, нақты жағдайларға сәйкес келмейді. Осы себепті Гросс моделінің оңайлылығын ескере отырып, мақсатты функцияны аппроксимациялау және алғашқы жуықтауда нәтижелерді алу үшін ғана пайдаланылады [68].

[69] зерттеуде **Грищук Р. В.** ақпараттық салаға кибершабуылдар туралы сипатталған. Кибершабуылдар кезінде қаскүнемдің мүмкіндіктерін бағалау кибершабуылдарды талдаудың ойын әдістерін пайдалана отырып жүргізіледі.

Автор ақпараттық жүйелерге кибершабуылдардың $A\,n$ ойыншысының одақсыз кибершабуылын қарастырған:

$$A = \left\langle N, \{x_i\}_{i \in N,} \{f_i(x)_{i \in N}\} \right\rangle, \tag{1.16}$$

мұнде $n-$ кибершабуыл ойыншыларының саны, оны $N, n \in \{N\}, N = \{1,2,...,n\}$ жиынында анықталған;

$i-$ кибершабуыл ойыншысының нөмірі, $i \in \{N\}$;

$x_i - i$-ші кибершабуыл ойыншысының стратегиясы, $x_i \in \{X_i\}$;

$f_i(x)-$ x кибершабуылдың i-ші кибершабуыл ойыншысына A төлем жасау, егер n ойыншы өз стратегияларын таңдаса, $x \in \{X\}$.

i- ші кибершабуыл ойыншының табысты кибершабуыл үшін төлем квадраттық функция түрін береді:

$$f_i(x) = xM^{(i)}x^T, \tag{1.17}$$

мұнда $M^{(i)}$ – симметриялық скалярлы квадраттық матрица;

x^T – баған- векторы.

$i-$ші ибершабуыл ойыншысы үшін кибершабуыл мақсаты $x_i \in X_i$ стратегиясын таңдау, қалыптасқан жағдайларда, жүзеге асырылған табыс жоғары болуы үшін, атап айтқанда :

$$f_i(x) \to \max. \tag{1.18}$$

Бұл модельде инвестициялардың оңтайлы шешімді таңдауға әсері ескерілмеген, алайда зерттеушілер әзірленген ойын талдау әдістері жеке және топтық кибершабуылдарды бағалауға мүмкіндік беретінін көрсетеді. Бұл ақпараттың кибершабуылдардан ақпараттық салаға қорғалу деңгейіне кепілді және сенімді баға алуға мүмкіндік береді.

О.Е. Архиповтың [70, 71] жұмыстары тәуекелдерді бағалау және ақпараттық қауіпсіздікке инвестициялардың тиімділігін зерттеу үшін «шабуыл-қорғау» экономикалық-құндық модельдерін қолдану мәселелерін зерттейді.

Шабуылдаушы тараптың A (қаскүнем) B тарапқа тиесілі кейбір ақпараттық ресурсқа I қатысты қатерлерді T жүзеге асыруы кезінде туындайтын жағдай қаралды.

$D-A$ шабуылдаушы тараптың T қатерлерді жүзеге асыруға арналған шығындарының жалпы құны, $g-$ бұл ретте алынған «ұтыс», оның шамасы қаскүнемдер үшін I ресурстың құндылығымен байланысты болады деп санайды. Бұл жағдайда B тараптың (I ресурс иесі) келтірген шығын, атап айтқанда оның иесі тұрғысынан ресурстың құны q ретінде бағаланады, ал іске асырылған қорғау шаралары жиынтығының жалпы құны c-ке тең.

Осы мәліметтер негізінде ақпараттық тәуекелдерді есептеу үшін қолданылатын ықтималдық сипаттамаларды сараптамалық бағалаудың

логикалық - эвристикалық схемасын құруға болады. T қатерді табысты жүзеге асырылған жағдайда қаскүнемнің таза пайдасы $Q = g - D$ құрайды.

Егер A шабуылдаушы тарап үшін I ресурстың g құндылығы елеулі болса, атап айтқанда, егер $g >> D$ болса, қаскүнемдер осы қатерді жүзеге асыру үшін кез келген мүмкіндіктерді пайдалануға тырысады деп болжауға болады. Керісінше, g аз мәндер үшін T қатердің пайда болуының экономикалық себептері іс жүзінде жоқ: $Q = 0$ болған жағдайда (немесе $g = D$) ресурстарға шабуыл жасау орынсыз болады, бұл жағдайда $P_t = 0$. $g < D$ үшін T қатерді жүзеге асыру әрекеті экономикалық мағынаны жоғалтады. Осы пікірлер негізінде келесі қатынас ұсынылды:

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g}, \tag{1.19}$$

T қатерді белсендіру (туындау) ықтималдығының болжамды (бағдарлы) мәндерін бағалау үшін пайдаланылуы мүмкін. Жалпы алғанда, T қатерді жүзеге асыру ықтималдығы – бұл келесі нәтижеден алынды:

$$P_T = P_t P_v, \tag{1.20}$$

мұнда P_v – қаскүнем I ақпараттық ресурсты қамтитын ақпараттық жүйенің (АЖ) осалдығын сәтті пайдалану ықтималдығы.

P_v ықтималдықтың мәні АЖ-нің қорғалу дәрежесіне байланысты, ол өз кезегінде ақпаратты қорғау жүйесіне c инвестициялардың көлеміне байланысты, бұл белгілі бір жуықтау арқылы қатынаспен ескеріледі:

$$P_v = \frac{q}{q + sc}, \tag{1.21}$$

мұнда s – коэффициент, ол ақпарат қорғау жүйесіне c инвестициялар тиімділігінің деңгейі анықталады, атап айтсақ: c инвестициялардың бір көлемі жағдайында s мән неғұрлым көп болған сайын, P_v ықтималдықтың шамасы соғұрлым төмен болады.

(1.21) формуладан АЖ-да критикалық ақпарат болмаған жағдайда (атап айтқанда $q = 0$) $P_v = 0$ ықтималдық анық көрсетілген. I ресурстың құны q жоғары немесе өте жоғары болғанда, бірақ ақпаратты қорғау жүйесін құру және жұмыс істеу шығындары төмен болғанда, атап айтқанда $q >> sc$, 2 ықтималдығы $P_v \to 1$. Егер I ресурстың иесі оны қорғауға жеткілікті назар аударса, q және sc мәндері шамалас, $P_v < 1$. $q = const$ кезінде P_v ықтималдықтың жалпы мәні ақпаратты қорғау жүйесіне c инвестициялар деңгейінің төмендеуімен өсуде және керісінше, олардың көлемінің өсуімен ұлғаюда. (1.19), (1.21) формулалар оңтайландыру схемасын құруға мүмкіндік береді, ол бойынша ұйымның ақпаратты қорғау жүйесіне инвестициялардың тиімділігі мен орындылығы туралы қорытынды жасауға болады.

Ол үшін [71, p.372] болжанған, $P_v = 1$ ұйымның ақпаратты қорғау жүйесіне нөлдік инвестициялау кезінде және шығу ақпараттық тәуекелі $R_1 = P_t q$ құрайды.

Ақпаратты қорғау жүйесіне c қаражат мөлшерінде инвестициялау (осы құралдардың қорғау қажеттіліктеріне арналған тиімді шығындары жағдайында) осалдықтың табысты орындалу ықтималдығы 1-ден аз болатынына әкеледі, атап айтқанда $P_v < 1$.

Бұл жағдайда қалдық тәуекел $R_t = P_t P_v q$ тең болады, $R_1 - R_t = P_t q - P_t P_v q = (1 - P_v) P_t q -$ алдын-алған шығын шамасы, ал $\Delta_R = R_1 - R_t - c = (1 - P_v) P_t q - c -$ тиісті «пайда».

Экономикалық-құндық модель экономикалық тенденцияларды ескере отырып, ақпараттық тәуекелдерді басқарудың нақты механизмдерін пайдалануды талап ететін, ақпараттық қауіпсіздік қажеттіліктерін, ұйымның ақпараттық жүйесінің қорғалу деңгейінің нақты көрсеткіштерін талдау нәтижелеріне негізделеді, содан кейін ақпаратты қорғау жүйесіне инвестициялардың оңтайлы көлемін бағалауды жүргізу кезінде неғұрлым объективті нәтижелерге қол жеткізуге үміттенеді.

«Шабуыл – қорғау» экономикалық-құндық модельдері нақты ұйым туралы айөын ақпараттың негізінде осы ұйымның ақпараттық қауіпсіздігіне инвестицияланған қаражаттың көлемі бойынша жеткілікті екендігін тексеруге мүмкіндік береді.

Левченко және бірлескен авторлар [72-75] мақсатты функцияны пайдалануды қарастыратын математикалық модель ұсынды

$$i(x; y),$$

мұнда i – жоғалған ақпарат құнының жалпы санына жатқызылған;

x және y – i шабуыл ресурстары, сәйкесінше, қорғау.

Бұл функция жалпы мағынада келесідей түрде беріледі:

$$i(x, y) = \sum_{k=1}^{l} i_k(x, y) = \sum_{k=1}^{l} g_k p_k q_k(x, y) f_k(x, y), \qquad (1.22)$$

мұнда $k = \overline{1, l}$ – нысан номері;

g_k – нысандағы ақпарат көлемі;

p_k – нысанға шабуыл жасау ықтималдығы;

$q_k(x; y)$ – k-ші нысанға x ресурстар шабуылының орналасу ықтималдығының тығыздығы;

$f_k(x; y)$ – жоғалған ақпарат үлесінің x және y арақатынасына тәуелділігі, оны x және y берілген мәндерде ақпаратты жоғалту ықтималдығы ретінде қарастыруға болады.

$f_k(x, y)$ тәуелділік есебінде функциялардың екі класы ұсынылады:

дәрежелік $$f(x, y) = \frac{\alpha (x / y)^n}{b(x / y)^n + c}, \qquad (1.23)$$

көрсеткіштік $$f(x, y) = d(1 - e^{-m(x/y)^n}), \qquad (1.24)$$

мұнда α, b, c, d, n, m параметрлері оң мәндерді қабылдайды және қисықтардың жағдайы мен көлбеуін анықтайды.

$2\,q(x) = Nx^n e^{-h^2x^2}$ түрінде $q(x)$ тәуелділіктің екі ықтимал түрі ұсынылған [72]:

Максвелл үлестірілуі:

$$q_M(x) = Nx^2 e^{-h^2x^2} \tag{1.25}$$

және Релей үлестірілуі:

$$q_p(x) = Nxe^{-h^2x^2}, \tag{1.26}$$

мұнда N – қалыпқа келтіру коэффициенті;

n, h – тұрақтылар, олар тәуелділіктің максимум жағдайын және оның асимметрия дәрежесін анықтайды.

Осы үлестірімдерді салыстыруда олардың маңызды айырмашылығы – $\tilde{x} > 0$ бастапқы аймақтағы $q_M(x)$ үшін дөңес төмен, ал $q_p(x)3$ үшін жоғары бағытталған.

Келтірілген мәндер компания немесе оқу орнының басшыларына бөлінген қаражаттың жеткіліктілігі немесе оларды ұлғайтудың орындылығы туралы қорытынды жасауға мүмкіндік береді. Бұл, әрине, $i(x, y)$ рұқсат етілген шамаларға байланысты , олар өз кезегінде, топ-менеджердің субъективті бағасы және оның тәуекелге бейімділігі тұрғысынан анықталады.

Сондай-ақ, қазір киберқауіпсіздікті инвестициялау үшін ойын теориясының негізінде жаңа модельдер жасауда. Осындай модельдердің бірі - Ахметов-Малюков моделі.

Ахметов-Малюков моделі [76] киберқауіпсіздік жүйесіне өзара инвестициялау стратегияларының (мысалы, компания және ЖОО үшін) моделін сипаттайды. Бірінші одақтас-ойыншының таза стратегиясы $u : T \cdot [0,1] \cdot [0,1] \to [0,1]$, функциясы деп аталады, ол $(t, (z_1(0), z_2(0)))$ ақпарат (позиция) жағдайына қойылатын $u(t, (z_1(0), z_2(0))) : 0 \le u(t, (z_1(0), z_2(0))) \le 1$ мән, мұнда u – бірінші инвесторды басқару параметрі; t – уақытша параметр; z_1 – бірінші инвестордың қаржы ресурсының шамасы; z_2 – екінші инвестордың қаржы ресурсының шамасы. Қарсылас - ойыншының хабардарлығына қатысты (позициялық ойын схемасы шеңберінде) кез келген ақпарат негізінде қарсылас ойыншы өзінің басқару әсерін $u(t)$ таңдайтынына баламалы ешқандай болжамдар жасалмайды.

Кез келген t уақыт кезеңі үшін шарттар орындалады:

$$\alpha_1(t) = \alpha_1;\ \alpha_2(t) = \alpha_2;\ \beta_1(t) = \beta_1;\ \beta_2(t) = \beta_2;\ r_1(t) = r_1;\ r_2(t) = r_2.$$

Қабылданды:

$$q_1 = (1 - \beta_1) \cdot (a_1 + r_1) - 1;$$
$$q_2 = (1 - \beta_2) \cdot (a_2 + r_2) - 1, \tag{1.27}$$

мұнда α_1 – бірінші инвесторға екінші инвестордың қаржы ресурсы үшін пайыздық төлемді айқындайтын коэффициент;

α_2 – бірінші инвестордың екінші инвесторға қаржы ресурсы үшін пайыздық төлемді айқындайтын коэффициент;

β_1 – бірінші инвестордың екінші инвесторға қарызын өтеу үлесін айқындайтын коэффициент;

β_2 – екінші инвестордың бірінші инвесторға қарызын өтеу үлесін айқындайтын коэффициент;

r_1 – екінші инвестордың бірінші инвесторға қаржы ресурсын қайтару үлесін айқындайтын коэффициент;

r_2 – бірінші инвестордың екінші инвесторға қаржы ресурсын қайтару үлесін айқындайтын коэффициент;

q^* – теңгерімділік сәулесін анықтайтын коэффициент.

Ақпараттық жүйелердің киберқауіпсіздік жүйесіне, атап айтқанда ҚОЖ-не өзара инвестициялау бойынша шешімді қолдау жүйесінің модулі үшін [76] модель ұсынылған. Модель инвестициялаудың нәтижелерін болжауға және инвестициялық процесті басқару стратегиясын табуға мүмкіндік береді. Қолданыстағы шешімдерге қарағанда, ұсынылған модель ҚО-дың қорғалған жүйесін құрудың инвестициялық процесіндегі стратегияларды таңдау кезінде айқын ұсыныстар береді. Егер болжам қанағаттанарлықсыз болған жағдайда, тараптар үшін қолайлы қаржылық нәтижеге қол жеткізу мақсатында инвестициялау процесінің параметрлерін икемді түрде түзетуге болады [76].

Киберқауіпсіздік жүйелері үшін инвестициялау стратегияларының математикалық модельдерін талдау негізгі құралдар мен күштер ақпараттық жүйелерді қорғау үшін инвестициялар мөлшерін анықтау мәселелеріне қолданылатынын көрсетті (кесте 1).

Кесте 1 – Киберқауіпсіздікке инвестициялаудың математикалық модельдерін талдау және алынған салыстырмалы сипаттамасы

Салыстыру критерийлері	Ақпараттық қауіпсіздік және киберқауіпсіздік жүйесінде инвестициялау стратегияларының математикалық модельдері					
	Гордон-Лоеб моделі	Вухен-Шим моделі	Архипов моделі	Левченко-Прус моделі	Задирак моделі	Ахметов-Малюков моделі
Динамикалық режимде оңтайлы шешімді есептеу	-	-	+	+	-	+
Объектілердің осалдығын есепке алу	-	-	+	+	-	-
Ресурстарды үлестіруді оңтайландыру	+	+	-	+	-	+
Қорғау құралдарын есепке алу	+	+	+	+	+	-
Шабуыл құралдарын есепке алу	-	-	+	+	-	-
Оң және теріс әсерлердің айырмашылығы	-	+	-	-	-	-
Әрбір қорғау құралының құнын есепке алу	-	-	+	-	-	-

Сонымен қатар, қолданыстағы модельдер құқық бұзушы ақпараттық қауіпсіздіктің қосымша инвестицияларына әрекет ете отырып, өзінің кибершабуылдар тактикасын қалай өзгертетінін сирек ескереді. Келтірілген шығынды сандық бағалау, қатерлер мен осалдықтың пайда болу ықтималдығы сияқты модельдер үшін деректерді алу кезінде қиындықтар бар.

Бірінші тарау бойынша қорытындылар

Диссертациялық жұмыстың бірінші тарауында:

– онлайн-білім беру, оның ішінде синхронды, асинхронды, қашықтықтан және аралас оқыту модельдеріне талдау жасалған. Қашықтықтан оқытуды ұйымдастырудың әртүрлі бұлтты-бағытталған тәсілдері сипатталған. Қызметтер мен ресурстар тұрғысынан жоғары оқу орындары үшін «академиялық бұлтты» пайдаланудың артықшылығы негізделеді, ол экономикалық тұрғыдан мүмкін болатындай модельдердің орналасуы мен құрылымын қамтамасыз етуі керек;

– қашықтықтан оқыту жүйесінің айналымындағы ақпараттық ағындарды бақылау мен өңдеудің қазіргі, сондай-ақ жаңа перспективалы механизмдерінің кешенді өзара іс-қимылының тиімділігін арттыруға қабілетті жоғары оқу орындарының қашықтықтан оқыту жүйесіндегі ақпараттық ағындарды (АА) ұйымдастыру құрылымы ұсынылды;

– әр түрлі ақпараттандыру нысандары үшін, соның ішінде ЖОО-ның қашықтықтан оқыту жүйесінде қолданылатын, виртуалдық бұлттық ресурстар мәселелерінің функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету сұрақтары зерттелді;

– ВБР-дың функционалды тұрақтылығы мен киберқауіпсіздігіне басқарудың күрделі нысандарының сенімділігі мен қорғалуын арттыру проблемаларын шешудің жүйелік тәсілі негізінде қол жеткізілетіні көрсетілген;

– ақпаратты қорғау жүйесіне және ақпараттандырудың әртүрлі нысандарының киберқауіпсіздігіне, оның ішінде ЖОО-н қашықтықтан оқыту жүйесіне инвестициялаудың тиімділігін бағалау үшін қолда бар модельдерге талдау жасалды. Қарастырылған модельдердің көпшілігінің кемшілігі-киберқауіпсіздік және қорғау жүйелерінде қаржылық инвестициялар стратегияларын қалыптастыру бойынша нақты ұсыныстардың болмауы;

– шешім қабылдауды қолдаудың компьютерлік жүйелері үшін жаңа модельдерді құру қажеттілігі негізделген, ол ҚОЖ-нің киберқауіпсіздігін және ақпаратты қорғауға қаржылық инфестициялардың оңтайлы стратегияларын табуға мүмкіндік береді;

– қашықтықтан оқыту жүйелерінің киберқауіпсіздігін инвестициялау мәселелеріндегі шешім қабылдауды қолдау жүйелері инвестициялаудың ұтымды стратегиясын табуға мүмкіндік беретін ойын теориясының математикалық модельдерін қолдану негізінде құрылуы мүмкін.

2 ҚАШЫҚТЫҚТАН ОҚЫТУ ЖҮЙЕСІНІҢ АҚПАРАТТЫҚ ЖЕЛІЛЕРІНДЕГІ ЖӘНЕ ВИРТУАЛДЫҚ БҰЛТТЫҚ РЕСУРСТАРЫНДАҒЫ КИБЕРҚАТЕРЛЕРДІ МОДЕЛЬДЕУ

2.1 Қашықтықтан оқыту жүйесінің ақпараттық желілерінің киберқатерін анықтау және оларды қорғау бойынша қарсышараларды таңдау әдісі

Диссертациялық жұмыстың 1.2 бөлімінде талданған қашықтықтан оқыту жүйесінің функционалды тұрақтылығын құру тұжырымдамасына сәйкес киберқатерлермен қашықтықтан оқыту жүйесінің ақпараттық қауіпсіздігі мен киберқауіпсіздігін қамтамасыз ету мәселелері зерттелді. Ол үшін зерттеу аясында қашықтықтан оқыту жүйесінде киберқатерді анықтау әдісі жетілдірілді.

Қашықтықтан оқыту жүйесіне жасалған кибершабуылдар [24, 26, 30, 32,] ақпараттың жоғалуына, жабдық пен аппараттық құралдардың істен шығуына, желінің пайдаланушылары мен иесіне келтірілетін едәуір материалдық және моральдық шығындарға әкеледі. Кибершабуыл көбінесе қашықтықтан оқыту жүйесіндегі – оның ақпараттық желілерінде немесе оларды қорғау жүйелерінде әлсіз орындар (осалдықтар) болуының салдары. Бұдан әрі ақпараттық желілер(АқЖ) деп қашықтықтан оқыту жүйесіндегі ақпараттық ағындарды беру арналарын түсінетін боламыз. АЖ (ақпараттық жүйелер) мен ЖАЖ (жасанды нейрондық желілер) аббревиатурасын ақпараттық желілермен (АқЖ) шатастырмауды өтінеміз.

Атап айтқанда, қашықтықтан оқыту жүйесінің ақпараттық активтеріндегі немесе оның ақпаратты қорғау жүйесіндегі әлсіздік осалдық деп аталады, ол белгілі бір киберқатерді (КрҚ) жүзеге асыру мүмкіндіктеріне әкеліп соқтырады. Сондықтан негізгі киберқатерлерге қарсы тұру мақсатында қашықтықтан оқыту жүйесінің ақпаратты қорғау жүйесі келесі мәселелерді шешуі тиіс:

– абоненттердің (пайдаланушылардың) қашықтықтан оқыту жүйесінің ресурстарына немесе /және ақпараттық желілерге қол жетімділігін шектеу және бақылау;

– байланыс арналары бойынша сәйкес келетін ақпараттық ағындардың аясында берілетін деректерді қорғау жөніндегі функцияларды жүзеге асыру;

– қашықтықтан оқыту жүйесінде немесе/және ақпараттық желілерде болып жатқан барлық оқиғалар (оның ішінде кіріс және шығыс ағындар) туралы ақпаратты тіркеу, жинау, сақтау, өңдеу және беру;

– ақпараттық желі (ҚОЖ) пайдаланушыларының жұмыс мониторингін жүзеге асыру;

– тексерілген потенциальды қатерлер үшін жұмыс істеу ортасының жабықтығын қамтамасыз ету;

– потенциальды қатерді (мысалы, «бетбелгілерді» қамтитын немесе сыни қателерге әкелетін) қашықтықтан оқыту жүйесінің ақпараттық желілеріне бақылаусыз енгізуден қорғауды жүзеге асыру;

– ақпаратты қорғау жүйелерін меңгеру құралдарынан өзін-өзі қорғауды және зиянды потенциальды қатерді енгізу мен таратудан қорғауды жүзеге асыру;

– қашықтықтан оқыту жүйесінің ақпараттық ресурстарының қолжетімділігін қамтамасыз ету, мысалы, деректерді резервтік көшіру арқылы;

– жалпы қашықтықтан оқыту жүйесі үшін критикалық ресурстардың тұтастығын қамтамасыз ету және бақылау.

ҚОЖ-нің ақпараттық желілеріндегі желілік трафиктегі кибершабуылдарды немесе аномалияны анықтау– бұл $F(t)$ функциясының мәні кез келген *t* уақытта штаттан өзгеше болатын жағдайы [27, 77].

АқЖ-лер және ҚОЖ-не бағытталған көптеген ішкі және сыртқы кибершабуылдар жиындарын төмендегідей кортеждер түрінде ұсынуға болады [43–46]:

$$RCA = \langle EST, CE, SS_{ne}, SS_h, PP, O(NN) \rangle, \quad (2.1)$$

$$ICA_{l(m)} = \langle IST_l^{k-1}, CE, SS_{ne}, SS_h, PP, O^k(NN_m^k) \rangle, \quad (2.2)$$

мұнда $RCA, ICA_{l(m)}$ – сәйкесінше, жалпы ақпараттық желілер мен қашықтықтан оқыту жүйелеріне қашықтағы және ішкі шабуылдар;

k – қашықтықтан оқыту жүйесіндегі ресурстың критикалық деңгейі;

EST – ҚОЖ үшін киберқатердің сыртқы көзі;

IST_l^{k-1} – ҚОЖ үшін киберқатердің ішкі көзі;

CE – қашықтықтан оқыту жүйесінде қолданылатын желілік жабдық;

SS_{ne}, SS_h – ҚОЖ-дегі шабуылдарды тарату жолдарындағы АҚ және КҚ сервистері;

PP – АқЖ-дегі хаттамалар мен пакеттер;

O – ҚОЖ және АқЖ-дегі нысандарға қол жеткізу;

NN_m^k – ең жоғары деңгейдегі критикалық (k) ақпарат өңделетін төбе, мысалы, ҚОЖ-нің сервері;

l, m – төбелер номері.

[77–79] жұмыстарында баяндалған жалпы тәсілдер дискретті күйдегі шабуылдардың қатерін марковтық модель негізінде қашықтықтан оқыту жүйесіне бағытталған қатерлер мен шабуылдарды модельдеуге негізделген. Авторлардың жұмыстарында көрсетілгендей ағын модельдерінде уақыттың үздіксіздігі қосымша есепке алынады. Бұл авторлардың пікірінше, киберқатерлердің қажетті сипаттамаларын есептеу үшін мүмкіндік береді.

Алайда, [77–79] жұмыстарда көрсетілгендей, қатерлердің марковтық модельдері кез келген жүйенің күйін модельдеудің тиімді құралы, соның ішінде ақпараттық қауіпсіздікті басқару жүйелерінің, ақпаратты қорғау жүйелерінің, қашықтықтан оқыту жүйелері. Мұндай тәсіл диссертациялық зерттеудің негізгі міндеттерінің бірін шешуге, атап айтқанда, қашықтықтан оқыту жүйесіндегі ақпараттың құпиялылығына, тұтастығына және қол жетімділігіне

тұрақсыздандыратын әсерлердің санын тұрақты арттыру жағдайында сәйкес қарсы шараларды таңдауға жауап бермейді.

Осылайша, қатерлердің марковтық модельдерін қолдану міндеттерінің белгілі зерттеулеріне сүйене отырып, одан әрі диссертациялық жұмыста қашықтықтан оқыту жүйесінің киберқауіпсіздігін инвестициялаудың ұтымды стратегиясын таңдау алгоритмдері мен модельдер жиынтығымен қашықтықтан оқыту жүйесіне шабуыл қатерлерінің нақтыланған марковтық модельдерін құру есебі шешіледі. Есептің мұндай тұжырымы диссертацияның бірінші тарауының 1.4 бөлімінің 1–кестесінде келтірілген модельдердің көпшілігінің маңызды кемшіліктерін жояды, атап айтқанда «қорғау нысандарының осалдығын есепке алу» сияқты маңызды критерийлерді ескеруге мүмкіндік береді. Демек, бұл есепті шешу қашықтықтан оқыту жүйесін қорғалған және функционалды тұрақтылығын құру әдіснамасын жетілдіруге мүмкіндік береді [80].

Қашықтықтан оқыту жүйесіне шабуылдар қатерлерін модельдеу есебі қарастырылғандықтан, бұзушының жүйенің осалдығын пайдалану реттілігін ескеру қажет емес.

Қашықтықтан оқыту жүйесіне шабуыл қатері киберқатердің екі класымен (типтерімен) құрылсын. Қарапайым жағдайда технологиялық осалдықтармен байланысты қатерлер ескерілмейді. Мұндай қатерлер көптеген жағдайларда қашықтықтан оқыту жүйесінің ақпаратты қорғау жүйелерінің жойылуына әкеп соқтырады. Осылайша, қашықтықтан оқыту жүйесінде қолданылатын (j) бағдарламалық құралдарды жүзеге асырылумен байланысты (i) қателіктермен жасалатын осалдықтар ғана қарастырылған.

Қашықтықтан оқыту жүйесінің күйіне сәйкес келетін марковтық тізбекке кіретін оқиғалардың ағынын қарастырайық. Біз λ арқылы кіріс ақпараттық ағындардың қарқындылығын, ал S_{ij} жүйенің күйін, мұнда i, j – сәйкесінше қашықтықтан оқыту жүйесінің осалдығы деп белгілейміз. [78] сәйкес, марковтық тізбектегі оқиғалар арасындағы ауысулар лезде орын алады деп санайды. Сонда [24-26, 77, 78] жұмыстарына сәйкес, марковтық модельдің модификациясы туралы айта аламыз, ол графтағы күйлердің арасындағы ауысулар $P_{ij} \cdot \lambda.$ ретінде белгіленеді (сурет 7).

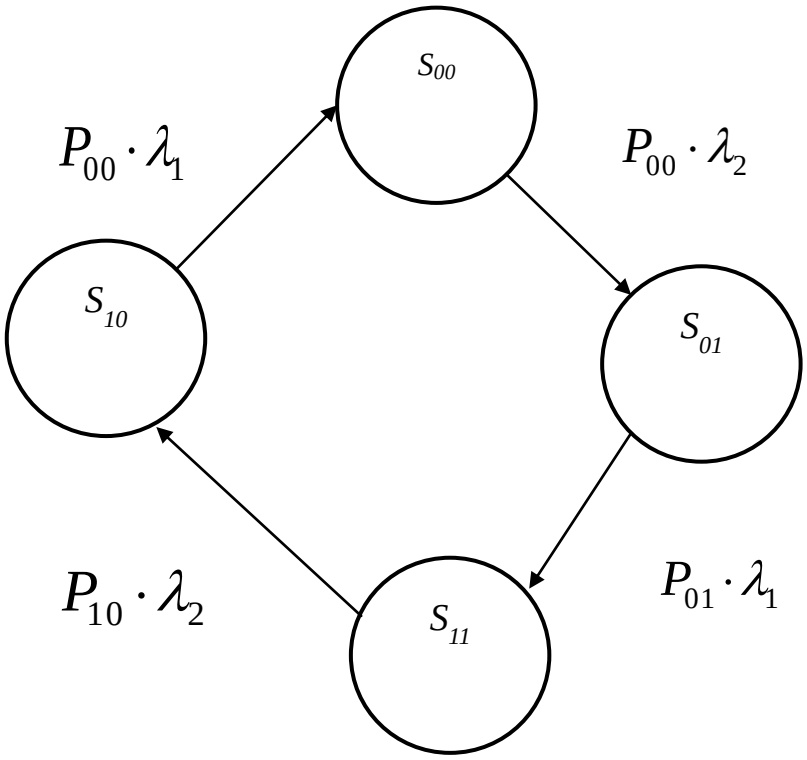
Сонда ҚОЖ-де нақты киберқатердің туындау қарқындылығын келесідей жазамыз:

$$\lambda_a = \sum_{S_i \in S_{(R-1)}} P_{S_i} \cdot \lambda_{S_i, S_R}, \tag{2.3}$$

мұнда $S_{(R-1)}$ – ҚОЖ күйінің жиыны, бұл киберқатерлердің болмауымен сипатталады және бұл ретте жүйе $P_{S_{(K-1)}}$; ықтималдығымен осы күйге келеді;

S_R – ҚОЖ-де нақты киберқатер туындайтын күй.

Сонда ҚОЖ-нің S_R - ден $S_{(R-1)}$-ге ауысуы, шабуыл салдарынан $\lambda_{S_{(R-1)},S_R}$ қарқындылығымен жүреді. 7–суретте көрсетілген граф үшін қарқындылықты келесідей анықтаймыз: $\lambda_a = P_{10} \cdot \lambda_2 + P_{01} \cdot \lambda_1$.



Сурет 7 – Киберқатерді жүзеге асыру нәтижесінде күйлер арасындағы ауысуларды модельдеу үшін ҚОЖ күйінің графын белгілеу мысалы

Ең қарапайым жағдайда ҚОЖ-нің тұрақты жұмыс істеу режимін қарастыруға болады, онда 7–суреттегі граф үшін нақты қатерлерді жою қарқындылығын келесідей анықтауға болады:

$$\mu_a = \lambda_a / (1 - P_{0a}) = (P_{10} \cdot \lambda_2 + P_{01} \cdot \lambda_1) / P_{11}. \quad (2.4)$$

Олай болса, ҚОЖ қауіпсіз жұмысқа дайын болу ықтималдығы кибершабуылдардың алдын алу ықтималдығы тұрғысынан келесідей анықтауға болады:

$$P_{0a} = (\mu_1 \cdot \mu_2 + \lambda_1 \cdot \mu_2 + \lambda_2 \cdot \mu_1) / ((\lambda_1 + \mu_1) \cdot (\lambda_2 + \mu_2)). \quad (2.5)$$

7–суретте көрсетілген граф кибершабуыл қатерлерін модельдеу проблематикасындағы тек қана жалпы көзқарасты көрсетеді, мысалы, қашықтықтан оқыту жүйесіне немесе кез келген компьютерлік жүйеге бағытталған. [79–84] жұмыстарында қарастырылған ережелерді ескере отырып, диссертация аясында шешілетін есептерге қатысты келесі постулаттарды тұжырымдауға болады:

1. Қашықтықтан оқыту жүйесіне бағытталған кибершабуылдардың қатерлі модельдері жалпы жағдайларда дұрыс болады, егер графта бар әрбір күйден барлық ағындар шығатын болса (атап айтқанда, жоғарыда қарастырылған ақпараттық ағындар) және осы ағынның қарқындылығы $\lambda_i, \quad i = 1,..., I.$ ретінде анықталған болса.

2. Қатерлерді модельдеу процесінде және қашықтықтан оқыту жүйелері үшін осы қатерлерге қарсы тұру стратегиясын жасаудың келесі кезеңінде марковтық тізбегінің математикалық аппаратын, атап айтқанда дискретті жағдайларымен және оқиғалар үшін үзіліссіз уақыт модельдерін қолдануға болады.

Қашықтықтан оқыту жүйесі үшін киберқатерді модельдеу кезінде стандартты қорғау өлшемдері (файрвол, антивирус, қашықтықтан оқыту жүйесінде есептік жазбаларды басқару, деректерді резервтеу жүйесі және т.б.) болған жағдайда, жүйеде бірден бірнеше осалдықтар пайда болу ықтималдығын елемеуге болады. Онда потенциальды осалдықтың қатері оның туындау туралы деректерді алғаннан кейін және жойылғанға дейін [82–86] бірден бәсеңдетіледі, ол кезде стохастикалық процесс үшін белгіленген граф күйі 8–суреттегідей ұсынуға болады.

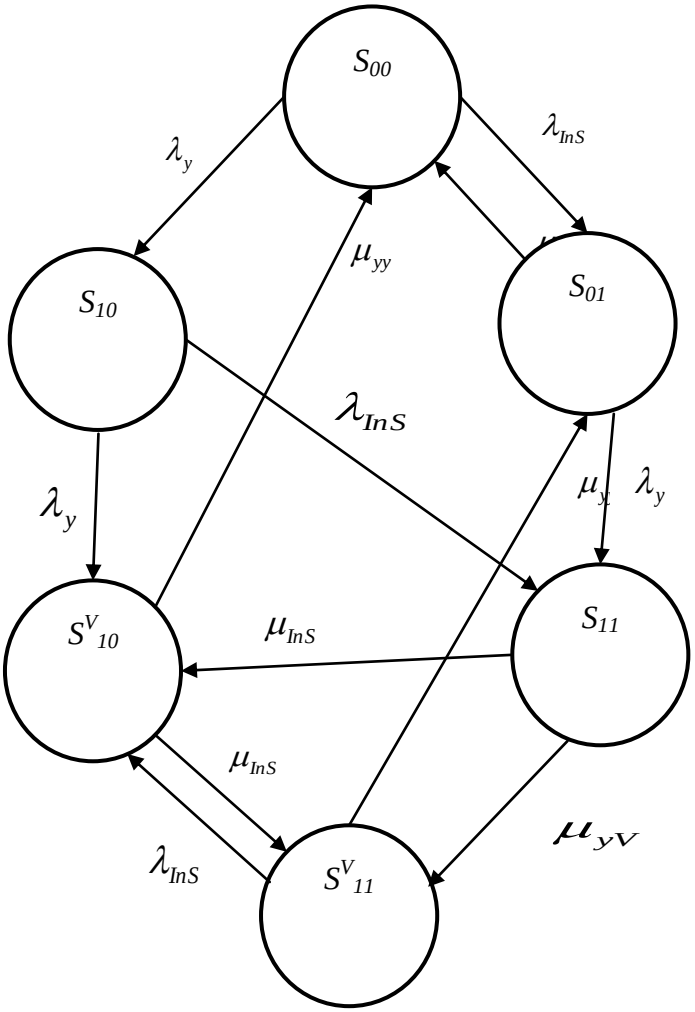
8 – суретте жүйенің күйі үшін төмендегідей белгілер қолданылады (граф төбелері): S_{00} – ҚОЖ-де жойылмаған осалдықтар жоқ; S_{10} – осалдық пайда болды, бірақ тиісті қорғаныс механизмдері әлі іске қосылмаған; $S^{V}{}_{10}$ – ҚОЖ-де осалдықтар анықталғанда, оның иесі оны қалпына келтіру процесін μ_{yy} қарқындылығымен бастайды және бұл ретте қашықтықтан оқыту жүйесінде ақпаратты резервтеуге негізделген мезанизм іске қосылды; S_{01} – осалдық ақпаратты қорғау құралдарында (АҚҚ) анықталған (мысалы, антивирус сигнатурасы ескірген), бірақ жойылмаған; S_{11} – ҚОЖ-де осалдықтар пайда болды, бірақ жойылмаған, АҚҚ-ы резерв функциясын әлі іске қоспады, өйткені осалдық әлі расталмаған; $S^{V}{}_{11}$ – осалдық расталды және оны қашықтықтан оқыту жүйесін қалпына келтіру процесі μ_{yy} қарқындылығымен басталады, алайда ақпаратты қорғау құралдарындағы осалдықтар жойылмаған [83–86].

Сонда жүйенің бір күйден екінші күйге ауысу процестерін сипаттайтын қарқындылықтарды келесідей белгілейміз: λ_y – ҚОЖ-де осалдықтар туындайтын қарқындылық; μ_{yV} – ҚОЖ- де осалдықтар анықталатын қарқындылық; μ_{yy} – ҚОЖ-де анықталған осалдықтарды ҚОЖ-нің персоналы немесе бағдарламалық қамтамасыз етуді әзірлеуші жоятын қарқындылық; λ_{InS} – ҚОЖ-нің АҚҚ-да осалдықтар туындайтын қарқындылық; μ_{InS} – ҚОЖ-нің АҚҚ-да анықталған осалдықтарды жоятын қарқындылық.

Олай болса, салынған графты есепке ала отырып, қашықтықтан оқыту жүйесінің қауіпсіздігі тұрғысынан қауіпсіз жұмысқа дайын болу ықтималдығын есептей аламыз, атап айтқанда P_{0yInS}:

$$P_{0yInS} = P_{00} + P_{01} + P^{V}{}_{10}, \qquad (2.6)$$

мұнда $P_{00}, P_{01}, P^{V}{}_{10}-$ ҚОЖ-нің $S_{00}, S_{01}, S^{V}{}_{10}$, күйлерінде болатын ықтималдықтар.



Сурет 8 – Потенциальды осалдықтың қатері ақпаратты қорғау құралдарына туындау туралы деректерді алғаннан кейін және жойылғанға дейін бірден бәсеңдейтін ҚОЖ-дегі стохастикалық процестің граф күйі

8 – суретте көрсетілген модель үшін шабуыл қатеріне (атап айтқанда $S_{00} \cup S_{01} \cup S^{V}{}_{10}$) қатысты киберқауіпсіздік параметрлері бойынша λ_0 істен шығуының туындау қарқындылығын келесідей анықтаймыз:

$$\lambda_{\text{o}} = \lambda_{y} \cdot (P_{\text{oo}} + P_{\text{o1}}) + \lambda_{InS} \cdot (P_{\text{o1}} + P^{V}{}_{\text{1o}}). \quad (2.7)$$

Содан кейін ҚОЖ-не бағытталған кибершабуылдар қатеріне қатысты параметрлерін қалпына келтіру қарқындылығын келесідей анықтауға болады:

$$\mu_{\text{o}} = \frac{\lambda_{y} \cdot (P_{\text{oo}} + P_{\text{o1}}) + \lambda_{InS} \cdot (P_{\text{o1}} + P^{V}{}_{\text{1o}})}{P_{\text{oo}} + P_{\text{o1}} + P^{V}{}_{\text{1o}}}. \quad (2.8)$$

Модельдеудің қорытынды кезеңінде есептеуге болады:

1) ҚОЖ-нің қауіпсіздік метрикасы бойынша істен шығу арасындағы уақыт:

$$T_o = 1/\lambda_0 ;$$

2) шабуылдан кейін ҚОЖ-н қалпына келтірудің орташа уақыты:

$$T^{V}{}_{o} = 1/\mu_{V},$$

мұнда $\mu_{InS} = \dfrac{\lambda_{inS} \cdot (P_{10} + P_{21}) + \lambda_{a} \cdot P_{01}}{P_{11} + P_{21}}$;

мұнда λ_{a} – қашықтықтан оқыту жүйесіне бағытталған шабуылдардың нақты қатерлердің туындау қарқындылығы; P_{11}, P_{21} – сәйкесінше S_{11}, S_{21} күйінің ықтималдығы, атап айтқанда 2 және одан да көп шабуыл қатерлерін жүзеге асыру мүмкіндігі болған кезде;

3) шабуылдан кейін ҚОЖ-нің қауіпсіздік жүйелерін қалпына келтірудің орташа уақыты:

$$T_{Oo} = T_{o} - T^{V}{}_{o}.$$

ҚОЖ үшін киберқатерді модельдеудің қарастырылған тәсілі зерттеудің келесі кезеңінде қорғау нысаны ретінде ҚОЖ-нің сенімді сипаттамаларын бағалауға ғана емес, сонымен қатар техникалық, ұйымдастырушылық және қаржылық сияқты оның құрамдас бөліктерін қоса қорғау стратегияларын құруға мүмкіндік береді. Осы шаралар жиынтығын жүзеге асыру қажетті уақыт кезеңінде қатерлерден ҚОЖ-нің қорғаныс деңгейін сақтауға мүмкіндік береді.

Қашықтықтан оқыту жүйелері үшін киберқатерді анықтаудың тұжырымдамалық және логикалық жүйесі келесі базалық модульдерді қамтуы тиіс, 9 – суретте көрсетілген:

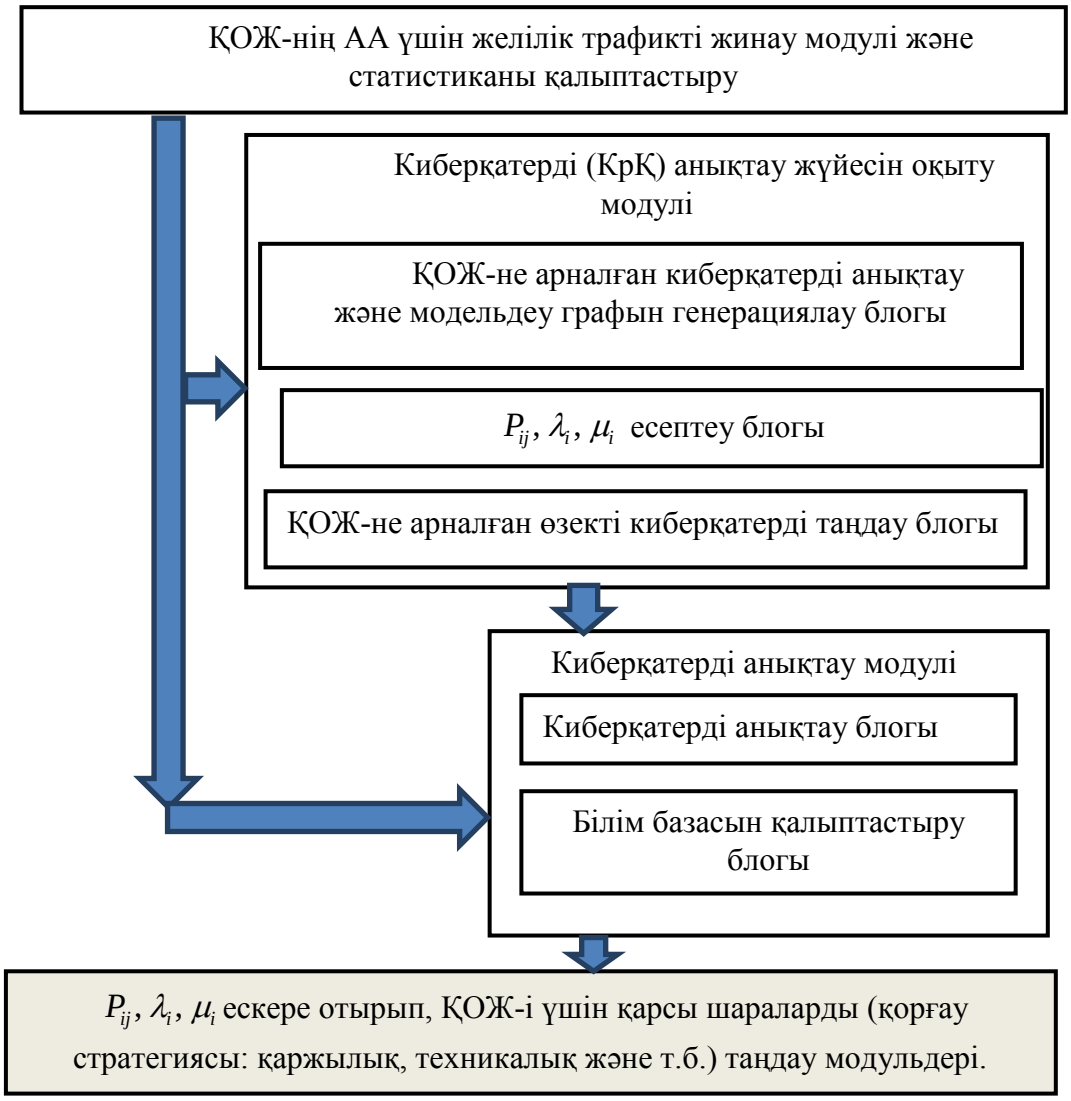
- трафикті жинау және статистиканы қалыптастыру модулі;
- киберқатерді (КрҚ) анықтау жүйесін оқыту модулі;
- киберқатерді анықтау модулі және хабарлама модулі.

Бірінші модульде ҚОЖ-нің ақпараттық желілерінің төбелері арқылы өтетін және киберқатер белгілерін көрсететін барлық трафикті ұстап қалу жүзеге асырылады, ал содан кейін оқыту модуліне жіберетін статистиканы қалыптастырады.

Оқыту модулінің негізгі есебі киберқатерді анықтау графын құру. Бұл графта, атап айтқанда шешімдерді қабылдауды қолдау жүйесінің немесе тану жөніндегі сараптамалық жүйенің білім базасында сақталатын барлық белгілі қатерлер туралы ақпаратты жинайды. Осылайша, ҚОЖ-нің ақпараттық желілеріндегі ақпараттық қауіпсіздік және киберқауіпсіздік саласындағы ағымдағы жағдайының толық көрінісі шығады [86–91].

Осының арқасында ҚОЖ-де анықталған оқиғалардың өзара тәуелділігін анықтау арқылы ықтимал жаңа киберқатерлер мен кибершабуылдарды болжауға мүмкіндік береді. Атап айтқанда, егер оқиға потенциальды кибершабуыл ретінде танылса, онда оның әсер ету зардабын жеңілдету үшін (мысалы, аппараттық-бағдарламалық қорғау құралдарын іске қосу есебінен) нақты шаралар қолдануға немесе алдын алу үшін сәйкес қаржылық немесе ұйымдық стратегиясын таңдауға немесе потенциальды қатерлі қатерді болдырмауға болады. Сондықтан киберқатерді анықтау графының негізгі

мақсаты - потенциальды кибершабуылдарды және олардың желі төбелеріне әсер ету нәтижелерін сипаттау.



Сурет 9 – ҚОЖ-нің ақпараттық желілісінде киберқатерді анықтау моделі

Киберқатерді анықтау графтарын (КрҚАГ) келесі өрнекпен сипаттауға болады:

$$G_{ГВКрУг} = (U, R), \tag{2.9}$$

мұнда $U-$ ҚОЖ-не бағытталған кибершабуыл графының төбелер жиыны;

$R-$ киберқатерді анықтау графының төбелерін қосатын бағытталған қырлар жиыны.

Кибершабуылдар туралы хабарлама көрсететін граф (КрШХКГ) төбелерінің үш типі болуы мүмкін:

$U_{dv}-$ осалдықты бейнелеу төбелері;

$U_{ruv}-$ осалдықты пайдалану нәтижесінің төбелері;

$U_{is}-$ бастапқы сатыдағы КрҚАГ-ның төбелері.

КрҚАГ-ның U граф төбелер жиыны ҚОЖ-нің потенциальды осалдығын көрсетеді және келесідей анықталады:

$$\boldsymbol{U} = \boldsymbol{U}_{dv} \cup \boldsymbol{U}_{ruv} \cup \boldsymbol{U}_{is}. \qquad (2.10)$$

$r \in R_{pe} \subseteq U_{dv} \times U_{rus}$ қырлардың жиыны U_{dv} төбелері U_{ruv}. төбелеріне жету үшін орындалуы тиіс жағдайды көрсетеді. $r \in R_{pos} \subseteq U_{ruv} \times U_{dv}$ қыры U_{ruv} төбелері үшін теңдік орындау үшін U_{dv} төбесі алынуы тиіс жағдайды көрсетеді:

$$\boldsymbol{R} = \boldsymbol{R}_{pe} \cup \boldsymbol{R}_{pos}, \qquad (2.11)$$

мұнда R_{pe} – осалдық алдыңғы төбеде және келесі төбенің осалдығын пайдаланған кезде нәтиже арасындағы өзара байланысты көрсететін қыр;

R_{pos} – алдыңғы төбедегі осалдықты пайдалану нәтижесі мен оны келесі төбеге пайдалану мүмкіндігі арасындағы өзара байланысты көрсететін қыр.

Ақпараттық желілерде киберқатерді анықтау модулі үшін кибершабуылдар туралы хабарламаларды көрсететін графтар (КрШХКГ) құрылады. Бұл граф осалдықтарды пайдалануды көрсететін төбелер мен осалдықтарды бейнелейтін төбелер жиынтығы болып табылады. КрШХКГ-ы уақыт белгілеріне сәйкес кибершабуылдан (КрШ) өтудің көптеген потенциальды жолдарын бір- бірімен төбелер арқылы құрайтын бағытталған қырлар жиынтығынан тұрады. Бұл ақпараттық желі төбелерінде желілік трафик туралы сәйкес хабарламаларды жасайды. Нәтижесінде сәйкес келетін төбедегі потенциальды киберқатерді көрсететін хабарламалар класын алуға болады. Осылайша, сәйкес келетін төбелерге хабарламаларды көрсететін КрҚАГ аламыз. Кибершабуылдың артуын бақылау үшін дереккөздің IP адресін және кибершабуылдың өту жолдарын қадағалау қажет.

Кибершабуыл туралы хабарламаларды көрсететін графты (КрШХКГ) төмендегідей сипаттауға болады:

$$G_{ГОКрАт} = (A, R, P).$$

A жиынтығы барлық хабарламалардың жиынын құрайды. Бұл жағдайда $a \in A$ хабарламалары жіберушінің IP адресін, алушының IP адресін, хабарлама типі мен уақыт белгісін қамтитын деректер құрылымы.

Барлық хабарламалар КрҚАГ-дағы (U_{dv}, U_{ruv}) екі төбесіне байланыстырылған. Бұл бағыт төбелерін көрсететін $map(a)$ функциясын пайдалануға байланысты:

$$map(a)$$
$$a \to \left\{ (U_{dv}, U_{ruv}) \middle| (a_{al} \in U_{dv\,node}) \wedge (a_{pr} \in U_{ruv\,node}) \wedge (a_{cl} = U_{dv\,vul}) \right\}, \qquad (2.12)$$

мұнда U_{dv} – қашықтықтан оқыту жүйесіндегі ресурстың осалдығын көрсететін төбе;

U_{ruv} – осалдықты пайдалану нәтижесін көрсететін төбе;

a_{al} – дереккөздің IP адресімен хабарлама;

U_{dvnode} – ҚОЖ-нің ақпараттық желісіндегі айқын түйінге сәйкес келетін төбе;

a_{pr} – тағайындау төбесінің IP адресімен хабарлама;

$U_{ruvnode}$ – U_{dvvul} -ге байланысты ҚОЖ-нің ақпараттық желісіндегі айқын түйініне сәйкес келетін төбе;

a_{cl} – осалдық класымен хабарлама;

U_{dvvul} – модельдеу процесінде қарастырылатын ҚОЖ-нің төбесіндегі осалдық.

Бағдарланған R қабырғалары өлшемдер шекті мәннен аспаған жағдайда (a, a') хабарламалар арасындағы корреляцияны білдіреді:

$$(a_{time} < a'_{time}) \wedge (a'_{time} - a_{time} < threshold\ value) \quad (2.13)$$

мұнда a_{time} – алдыңғы төбені көрсететін уақытша белгі;

a'_{time} – келесі төбені көрсететін уақытша белгі;

Содан кейін , аламыз:

$$\exists (U_{dv}, U_{ruv}) \in R_{pe} : (a_{pr} \in U_{ruvnode} \wedge a_{al} \in U_{ruvnode}). \quad (2.14)$$

Кибершабуыл туралы хабарламаларды көрсететін графтар P - кибершабуылдан өту маршруттарының жиынтығынан құралады.

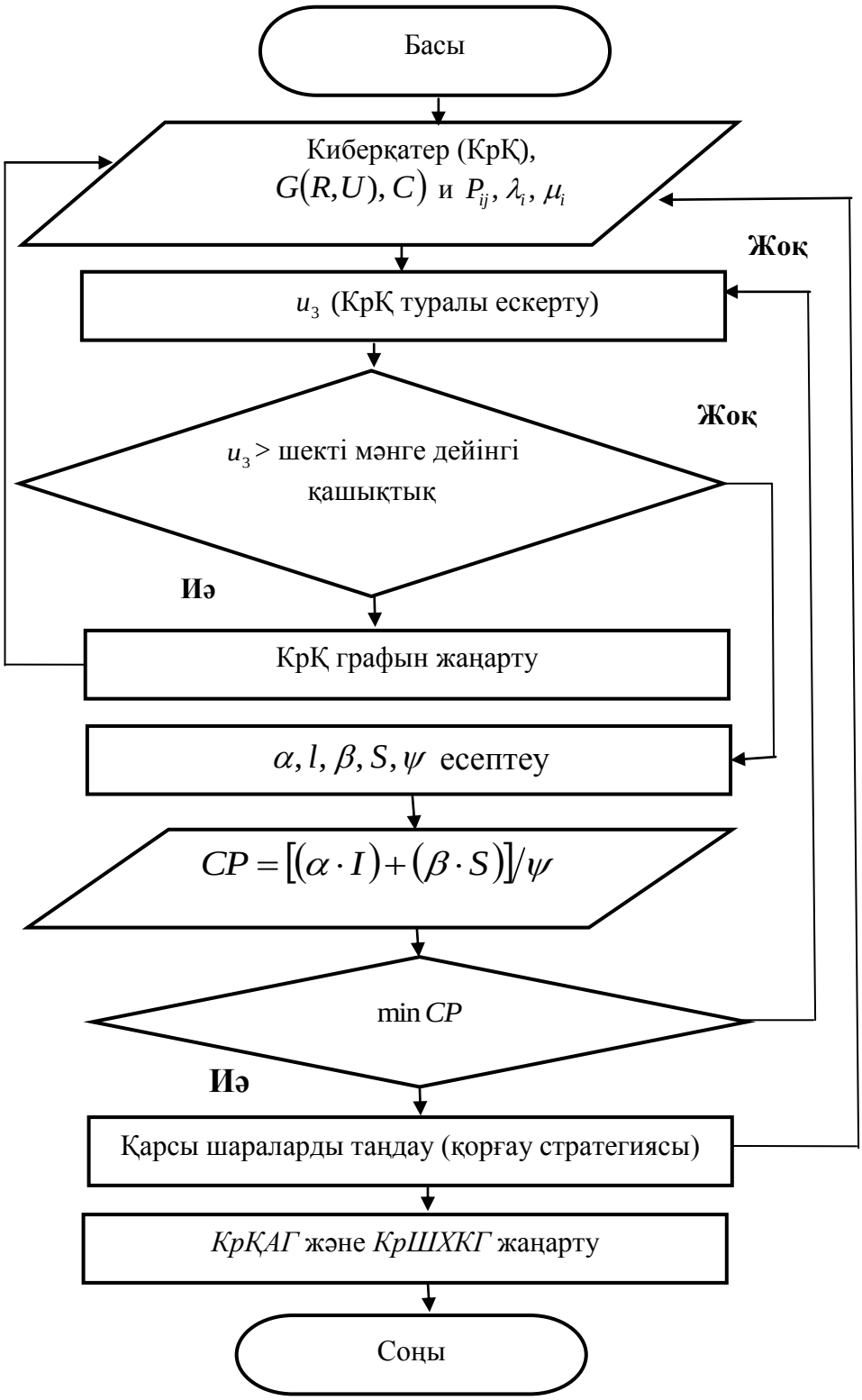
$M_i \subset P$ маршрут ҚАЖ-не бағытталған кибершабуылдың бір сценарийіне жататын жүйеге түсу ретіне байланысты хабарламалар жиынтығы.

КрШХКГ-да әрбір реттелген (a, a') жұбы киберқатерді анықтау графының екі көршілес төбесімен салыстырылады. Хабарламалардың сағаттық белгілеріндегі айырмашылық екіге тең деп қабылданды.

КрШХКГ-да хабарламалардың уақыт ретімен тәуелділігін көрсетеді. Бұл КрШХКГ-да хабарламаларды іздеу арқылы кибершабуылдар сценарийіне байланысты хабарламаларды табуға мүмкіндік береді (сурет 10).

КрШХКГ-да шабуылдан өту бағыттарының жиындар жиынтығы КрҚАГ-дағы бастапқы төбеден мақсатты (нысаналы) төбеге дейінгі барлық жолдарды сақтау үшін пайдаланылады. $M_i \subset P$ әрбір жолы КрШАГ және кибершабуылдан өтудің бірдей мақсатына тиесілі хабарламалар. Кибершабуылдар анықталғаннан кейін КМКЖ немесе ақпараттық желі үшін потенциальды киберқатерлерді одан әрі есте сақтау үшін КрҚАГ-ы жаңартылады.

Киберқатер туралы хабарламалар модулінде айқын қашықтықтан оқыту жүйесі үшін киберқатерді анықтау сценарийі үшін қарсы шара таңдау жүргізіледі. Кейін ШҚҚЖ-нің көмегімен ақпараттық желілерді басқару мақсаттарының динамикалық өзгеруі жағдайында әртекті дереккөздерден алынған мәліметтер негізінде қажетті түрдегі және қорғау деңгейі туралы шешім шығаруды іске асыру үшін. Қарсы шараларды таңдаудың мақсаты КМКЖ немесе ақпараттық желі төбелерін компрометациялаудан қорғау.



Сурет 10 – ҚОЖ-нің ақпараттық желісінің төбесін компрометациялануын болдырмау үшін киберқатерді тану және сәйкес қарсы шараларды таңдау әдісін жүзеге асыратын блок схема

Желілік қауіпсіздік осалдығының жағдайын бағалау және ақпараттық желінің ағымдағы конфигурациясын анықтау үшін кибершабуылдарды анықтау

графында ақпараттық қауіпсіздік, киберқауіпсіздік көрсеткіштерін пайдалану қажет. Графта (КрШХКГ) ҚОЖ-дегі осалдықтар туралы ақпараттардан тұрады.

Бастапқы немесе сыртқы төбелер үшін (атап айтқанда, түбірлік төбе, $U_{is} \subseteq U_{ruv}$), кибершабуылдың потенциальды дереккөзінің априорлы ықтималдығы бар. Графтың U_{is} төбесінің априорлық тәуекелінің ықтималдығын белгілеу үшін осалдықтар базасынан GU көрсеткіші пайдаланылады. GU мәніне, әдетте, жоғары ықтималдылық беріледі, мысалы, 0,75-тен 1-ге дейін.

Киберқатерді анықтаудың әзірленген әдісі үшін шабуылдың әсер ету зардабын бәсеңдету көрсеткішін енгізу ұсынылды, ол үшін қарсы шара мәліметтер базасында қарсы шаралар бойынша нұсқаулықтар жасалады:

$$Q = \{C_1, ..., C_n\}; \quad (2.15)$$

мұнда $Q-$ қарсы шара мәліметтер базасы, ол осалдықтар немесе кибершабуылдар анықталған кезде қашықтықтан оқыту жүйесінің иесіне қабылдауға ұсынылады;

$C-$ ҚОЖ-нің ақпараттық желі төбесінің компрометациялануын болдырмау үшін қарсы шаралар.

Әрбір қарсы шара $C \in Q$. Осылайша, қарсы шараларды жалпы келесі түрде жазуға болады:

$$C = (S, I), \quad (2.16)$$

мұнда $S-$ ресурстар мен жедел күрделілік тұрғысынан қарсы шараларды жүзеге асыру үшін қажет шығындар;

$I-$ өнімділіктің төмендеуі немесе «келеңсіз әсер» (интрузивтілік [88]), ол жаңа қарсы шараларды енгізу нәтижесінде ақпараттық желілердің абоненттеріне сезіледі. Бұл параметр 1-ден 10-ға дейінгі аралықта анықталады (жоғары балл жоғары құнды білдіреді деп санаймыз).

Егер қарсы шараларды КМКЖ немесе ақпараттық желіде қызмет көрсету сапасын төмендетпесе, интрузивтілік 0-ге тең. Осылайша, қарсы шаралар-қорғаныс құралдарын таңдаудың кешенді көрсеткішінің ең аз мәніне сәйкес келетін қарсы шараларды таңдау қажет.

Кибершабуылдан қашықтықтан оқыту жүйесін және қажетті қарсы шаралар таңдау қорғау мақсатына жету үшін кешенді көрсеткішті пайдалану ұсынылады:

$$CP = \left[(\alpha \cdot I) + (\beta \cdot S)\right] / \psi, \quad (2.17)$$

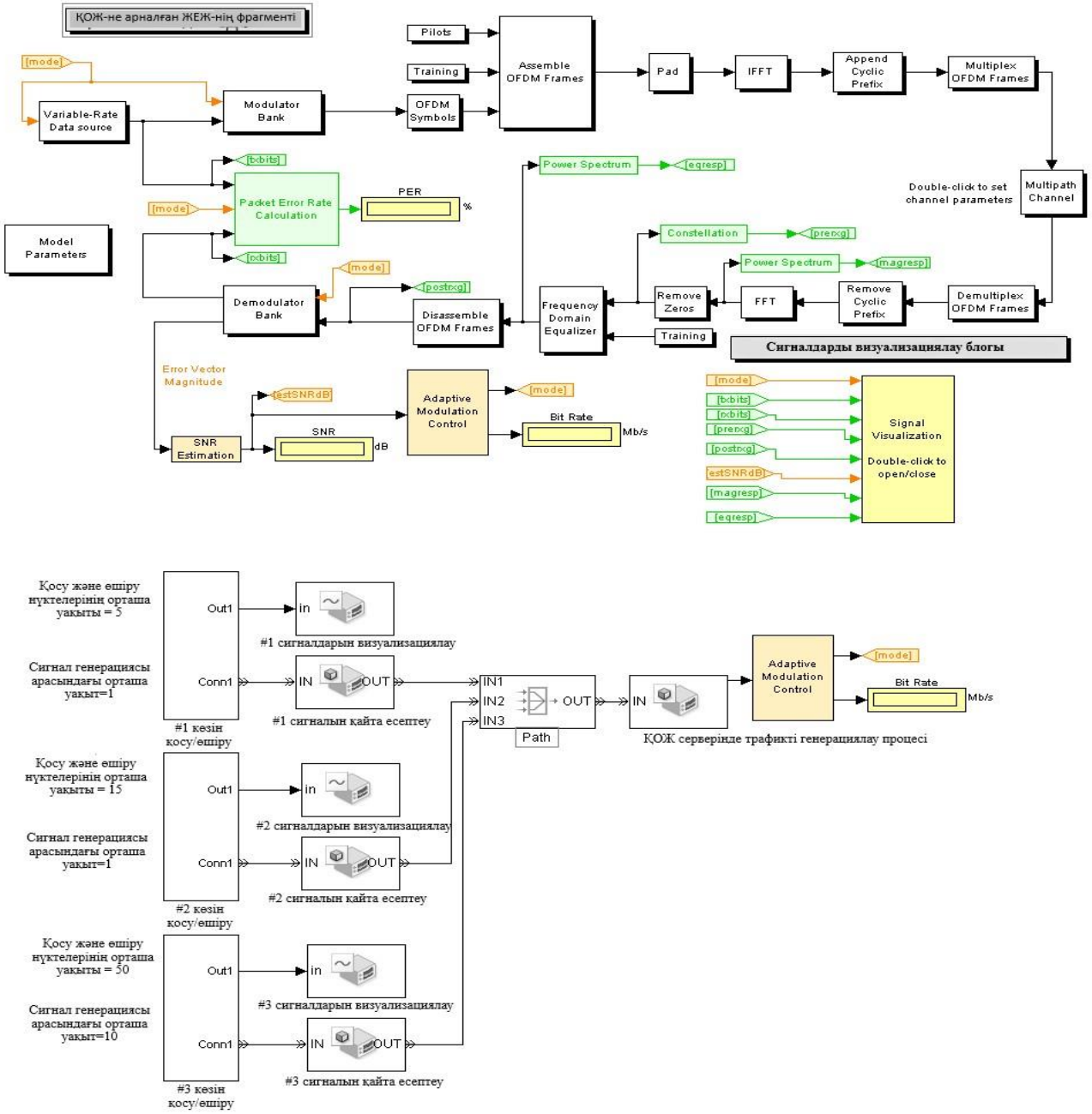
мұнда $\alpha, \beta -$ ақпараттық желінің жалпы өнімділігіне қарсы шаралар көрсеткіштерінің әсер ету сипаттамалары;

$\psi -$ нормалау коэффициенті.

Интеллектуалды ақпараттық желіде киберқатерді анықтаудың жетілдірілген әдісін пайдалану нәтижесінде киберқатерді өту жолын ажырату мүмкіндігі пайда болады. Бұл, өз кезегінде, шабуылдаушыға өз мақсатына жету үшін басқа балама жолдарды іздеуге мәжбүр етеді.

ҚОЖ үшін киберқатерді анықтаудың ұсынылған әдісін тексеру үшін бағдарламалық модульді тестілеу жүргізілді, ол [90, 91] жарияланымда сипатталған, сондай-ақ диссертациялық жұмыстың 3-тарауында оның кеңейтілген нұсқасы сипатталған.

Қашықтықтан оқыту жүйесінің ақпараттық желісінің сегменті үшін MATLAB ортасында имитациялық модельдеу барысында (сурет 11) ақпараттық желіге бағытталған қатерлер мен шабуылдарды тану кезінде қарсы шараларды таңдау алгоритмін жүзеге асыратын бағдарламалық модульді тестілеу жүргізілді. Модельдеу нәтижелері 2 – кестеде көрсетілген.



Сурет 11 – ҚОЖ-нің ақпараттық желісі сегментінің имитациялық моделі (Matlab)

Кесте 2 – Ақпараттық желі төбесінің компрометациялануын болдырмау үшін сәйкес қарсы шараларды таңдау, киберқатерді тану әдісін және бағдарламалық алгоритмді имитациялық модельдеу кезіндегі тестілеу нәтижелері

Кибершабуылдар класы	Жауап қайтару нұсқалары (С - қабылданатын қарсы шаралар)		
U2R	A=2, B=3, P_a = 0,54	A=1, B=1, P_a = 0,242	
	Шабуыл көзі төбесімен сессияны аяқтау (ШКТСА)	Абонентке хабарлама жіберу (АХЖ)	
R2L	A=1, B=3, P_a = 0,4-0,45	A=1, B=1, P_a = 0,192	
	ШКТСА	АХЖ	
DOS/DDOS	A=2, B=3, P_a = 0,6-0,65	A=1, C=2, P_a = 0,4-0,5	
	ШКТСА	АХЖ	
Wi Fi арқылы сыртқы шабуыл	A=3, C=3, P_a = 0,678	A=1, C=2, P_a = 0,4	A=1, C=1, P_a = 0,3
	Кіру нүктесін бұғаттау	Шабуыл жасайтын станцияға DOS-шабуылы	Жауаптың болмауы
Ақпараттық желі периметрі арқылы қашықттан шабуыл	A=3, B=4, C=2, P_a = 0,82	A=1, B=1, C=1, P_a = 0,224	A=1, P_a = 0,076
	Ақпараттық желілер серверіне қолжетімділікті бұғаттау	IP блоктау мақсатында қауіпсіздік сервистерінің конфигурациясын өзгерту	АЕЖ

ҚОЖ үшін ақпараттық желі төбесінің компрометациялануын болдырмау үшін сәйкес қарсы шараларды таңдау, киберқатерді танудың жетілдірілген әдісін тестілеу және имитациялық модельдеу нәтижелері көрсетті:

− ұсынылған тәсіл [30, 77–83] жұмыстарында сипатталған әдістермен салыстырғанда ақпараттық желіде қатерлерді анықтау бойынша шешім қабылдау кезінде есептеу күрделілігін 5-7%- ға төмендетуге мүмкіндік береді;

− ақпараттық желіде және қашықтықтан оқыту жүйесіндегі киберқатерді анықтаудың жетілдірілген әдісі ЖОО мен басқа да оқу орындарының қашықтықтан оқыту жүйесінің ақпараттық қауіпсіздігі мен киберқауіпсіздігі бойынша шешімдер қабылдауды қолдаудың жобаланатын және қолданыстағы жүйелері үшін қолданылуы мүмкін.

Ұсынылған тәсіл әртүрлі ақпараттандыру нысандары үшін, оның ішінде қашықтықтан оқыту жүйелері үшін қатерлерді тану жүйелерінде пайдаланылатын ұқсас шешімдермен салыстырғанда мынадай артықшылықтарға ие:

– әдіс әр түрлі сыни деңгейдегі ақпарат өңделетін, оның ішінде қашықтықтан оқыту жүйелері үшін де, көптеген төбелерден тұратын қорғау нысандарындағы ақпараттың қорғалу деңгейін бағалауға мүмкіндік береді;

– ақпараттық ресурстардың сындылық деңгейін ескере отырып, ЖОО-ның қашықтықтан білім беру жүйесінің ақпараттық желілерінің сегменттері мен төбелерінің саны бойынша бастапқы деректерді беруге болады;

– ақпараттық желілерді қорғау үшін қарсы шараларды бағалаудың жеделдігі қамтамасыз етіледі.

Алайда, сипатталған әдісті толық қолдану үшін айқын ақпараттық желі, қашықтықтан оқыту жүйесі және оның ақпаратты қорғау жүйесі үшін қатер графтарын салу қажет. Бұл ҚОЖ-н ұйымдастырудың ерекшелігі әр түрлі болуы мүмкін екендігіне байланысты. Мысалы, оқу орнының ауқымына және ондағы сәйкес ақпараттық ағынды ұйымдастыруға байланысты. Сондықтан диссертациялық жұмыстың 2.1 бөлімінде зерттеулердің қазіргі кезеңінде біз MatLab пакетін қолданумен және қашықтықтан оқыту жүйесінің ақпараттық желісі сегментін имитациялық модельдеумен шектелдік.

2.2 ЖОО-ның қашықтықтан оқыту жүйесінің бағдарламалық-конфигурацияланатын желілері үшін виртуалдық бұлттық ресурстарының киберқауіпсіздігін қамтамасыз ету модельдері мен алгоритмдері

Диссертацияның 1.3 бөліміндегі талдаудың нәтижесінде бағдарламалық-конфигурацияланатын желілер негізінде виртуалдық бұлттық ортаның функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету әдістемесін, ЖОО-ның виртуалдық бұлттық ресурстарының күйін бағалау, қорғау көрсеткіштерінің мониторингін және қарсы шараларды таңдау үшін модель құру қажет.

Зерттеу барысында виртуалдық бұлттық ресурстарына кибершабуыл жасау әсерін сипаттайтын модель жетілдірілді. Бұл модельдің қолданыстағылардан ерекшелігі - хабарлама корреляциясы графында (ХКГ) қабырғаларды тұрғызу үшін көрсеткіш пайдаланылады [52], онда жүйедегі көршілес төбелерден ($D(Alert)$ и $Alert$) хабарлама түсімдерінің арасындағы уақыт айырмашылығы есепке алынады:

$$T = D(Alert) \bigcup Alert, \tag{2.18}$$

Виртуалдық бұлттық жүйелерге шабуыл графы әзірленді, ол жүйенің барлық белгілі осалдықтары туралы ақпарат алуға мүмкіндік береді, сондай-ақ нақты уақыт режимінде жүйенің функционалды тұрақтылығы мен киберқауіпсіздік күйін көрсетеді. Бұл анықталған оқиғаларды корреляциялау жолымен мүмкін қатерлер мен шабуылдарды болжауға мүмкіндік береді.

Шабуыл графының сценарийін (ШГС) кортеж үлгісінде беруге болады:

$$SC_{ga} = \langle VR, ED \rangle, \tag{2.19}$$

мұнда VR – шабуыл графы (ШГ) төбелерінің жиыны;

ED – ШГ төбелерін байланыстыратын бағытталған қырлар жиыны.

ШГ төбелерінің үш типі болуы мүмкін:

NO_{co} – конъюнкция төбелері (осалдықты бейнелеу үшін);

NO_{di} – дизъюнкции төбелері (қаскүнем осалдықты пайдаланған нәтижесін белгілеу үшін);

түбірлік төбе NO_{ro} – (шабуыл сценарийінің бастапқы кезеңін белгілеу үшін).

ШГ төбелерінің жиыны VR келесідей анықтаймыз:

$$VR = NO_{co} \cup NO_{dt} \cup NO_{ro}. \quad (2.20)$$

$ed \in ED_{pre} \subseteq NO_{dt} \times NO_{co}$ қабырғаларының жиыны NO_{co} жету үшін қандай NO_{dt} орындалуы керек екенін көрсетеді. $ed \in ED_{post} \subseteq NO_{co} \times NO_{dt}$ қабырғасы NO_{co} төбелері орындалуы үшін U_{dv} төбесі алынуы тиіс күйін көрсетеді.

Содан кейін

$$ED = ED_{pre} \cup ED_{post}, \quad (2.21)$$

мұнда ED_{pre} – алдыңғы төбеде осалдықты пайдалану нәтижесі арасындағы өзара байланысты келесі төбе сол осалдықпен көрсететін ШГ-ның қабырғалары;

ED_{post} – алдыңғы төбедегі осалдықты келесі төбеге пайдалану нәтижесінің мүмкіндігі арасындағы өзара байланысты көрсететін қабырғалары.

Хабарламаны корреляциялау графын (ХКГ) келесі кортеж түрінде ұсынамыз:

$$G_{cev} = \langle AL, ED, SR \rangle, \quad (2.22)$$

мұнда $\{AL\}$ – $(Alert)$ барлық хабарламаларды қамтитын жиын.

$al \in AL$ хабарламасы - бұл дереккөз мен алушының IP-адрестерін, хабарлама түрін, сондай-ақ уақытша белгілерді қамтитын деректердің құрылымы;

SR – ХКГ-да шабуылдардың өту маршруттарының жиынтығы.

Әрбір хабарлама ШГС-да $(vr_c; vr_d)$ төбелері тең. Хабарламаларда виртуалдық бұлттық ресурстарына шабуылдар әсерінің жетілдірілген моделін көрсететін $map(al)$ функциясы қолданылады:

$$map(al): al \to \left\{ (vr_c, vr_d) \middle| \begin{array}{l} (al.sour.addr.alert \in vr_{c.host}) \wedge \\ (al.dest.addr.alert \in vr_{d.host}) \wedge \\ (al.alert.cl = vr_{c.vul}) \end{array} \right\}, \quad (2.23)$$

мұнда vr_c – осалдықты бейнелейтін төбе;

vr_d – осалдықты пайдалануды бейнелейтін төбе;

$al.sour.addr.alert$ – дереккөздің IP-адресімен хабарлама;

$vr_{c.host}$ – бұлттық ортадағы нақты төбеге сәйкес келетін төбе;

$al.dest.addr.alert$ – тағайындау төбесінің IP-адресімен хабарлама;

$vr_{d.host}$ – $vr_{c.host}$ байланысты виртуалдық бұлттық ортасындығы нақты төбеге сәйкес келетін төбе;

$al.alert.cl$ – осалдық класымен хабарлама;

$vr_{c.vul}$ – талданатын төбедегі осалдық;

c – осалдықтың индексі;

d – осалдықты пайдалану индексі.

Бағытталған қабырғалар, (al, al') екі хабарлама арасындағы корреляцияны көрсетеді, егер келесі өлшемшарттары ақиқат болса:

$$(al.time < al'.time) \wedge (al'.time - al.time < threshold \quad value), \tag{2.24}$$

мұнда $al.time$ – алдыңғы төбедегі уақытша белгімен хабарлама;

$al'.time$ – келесі төбеде уақытша белгімен хабарлама.

$$\exists (vr_c, vr_d) \in ED_{pre} : \wedge \begin{pmatrix} (al.dest.addr.alert \in vr_{d.host}) \wedge \\ (al.'sour.addr.alert \in vr_{c.host}) \end{pmatrix}. \tag{2.25}$$

$RO_i \subset SR$ маршруты бірдей шабуыл сценарийіне тиесілі хронологиялық тәртіпке байланысты хабарламалар жиынтығын көрсетеді.

Шабуыл графы қаскүнемнің әрекетін болжау үшін қолданылады. Оның негізінде бұлттық ортада қатерлерді талдау алгоритмі салынды (сурет 12).

Әрбір хабарлама үшін алгоритміне сәйкес шабуылдан өтудің бір немесе бірнеше RO_i маршруттары анықталады және қайтарылады. Басып кіруді анықтау жүйесінен алынған әрбір хабарлама үшін ХКГ-на жаңа төбе қосылады, егер ол болмаса. Бұл жаңа хабарлама үшін, ШГС-не сәйкес келетін төбеде $map(al)$ функциясының көмегімен табамыз. ШГС-дегі осы төбе үшін, оның NO_{co} типті төбелерімен байланысты хабарламалар корреляцияланады. Бұл ХКГ-да RO_i жолына қатысты жаңа төбелер жиынтығын құрайды немесе $RO_i + 1$ жаңа жол құрайды. Виртуалдық бұлттық ортаға қатерлерді талдау алгоритмінің соңында ШСГ-на сәйкес төбеге хабарлама атрибутын қосамыз. Алгоритм жұмысының нәтижесі виртуалдық бұлттық ортаға шабуылдың бір немесе бірнеше жолын алу болып табылады.

Сонымен қатар, зерттеу барысында виртуалдық бұлттық ресурстардың күйін бағалау моделі жетілдірілді. Модель (2.26)-(2.29) өрнектерімен сипатталған. Модель $(cm \in CM)$ қарсы шараларды таңдау үшін $(cm.ef)$ қарсы шарадан «Қызмет көрсету деңгейі туралы келісімге» (немесе $(Benefit(or \quad B))$), теріс әсерін сипаттайтын көрсеткіш, сондай-ақ ресурстар мен операциялық күрделілік тұрғысынан қарсы шараларды қолдану үшін қажетті шығындар көрсеткіші пайдаланылатынымен ерекшеленеді.

ВМ-ны бағалау үшін, функционалды тұрақтылығы тұрғысынан, ВМ-ның функционалды тұрақтылығының көрсеткішін пайдалану ұсынылды:

$$FS_{VM} = A_{VM} + A_{U_{VM}}, \tag{2.26}$$

мұнда $A_{U_{VM}}$ – ВБО-да виртуалдық машинаның осалдығын пайдалануды бағалау;

A_{VM} – ВМ-ның осалдығын бағалау.

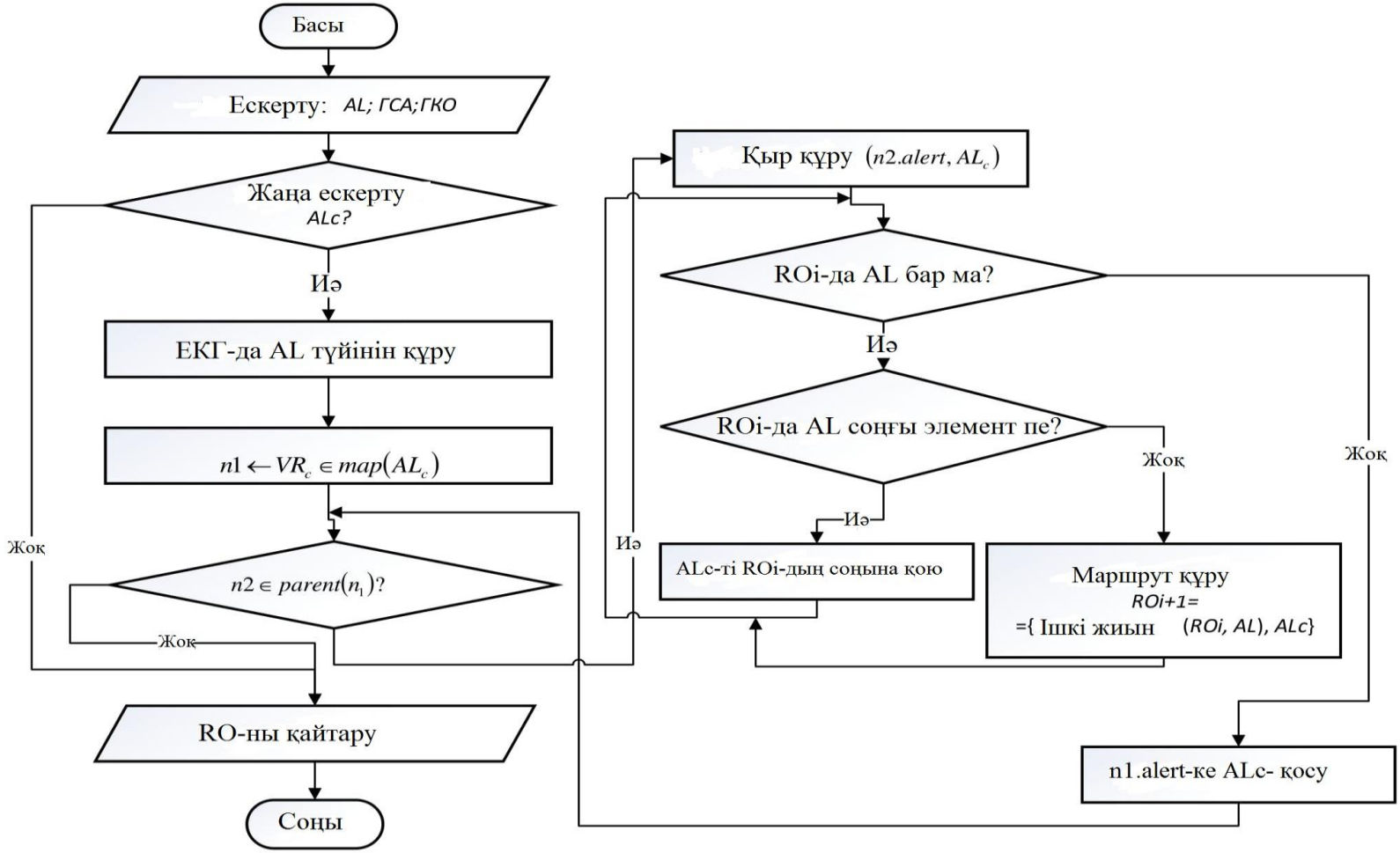
$$A_{VM} = \min\left\{10, \ln \sum e^{BL(vm)}\right\}, \tag{2.27}$$

деп қабылданды.

мұнда BL – нақты ВМ-ның әрбір осалдығы бойынша орташа базалық балл – vm.

ВМ-ның осалдығын пайдалануды бағалауды келесідей алуға болады:

$$A_{U_{VM}} = \left(\min\left\{10, \ln \sum e^{W(vm)}\right\}\right)\left(\frac{N_{(vm)}}{Q_{(vm)}}\right), \tag{2.28}$$



Сурет 12 – ВБО-дағы киберқатерді талдау алгоритмі

мұнда $W(vm)$ – нақты ВМ-ның осалдықтарының әрқайсысының осалдығын пайдаланудың орташа балы; $N_{(vm)}$ – ВМ ұсынатын қызметтер саны; $Q_{(vm)}$ – ВБО-ға ВМ-лар ұсынылуы мүмкін қызметтердің саны.

Атап айтқанда, A_{VM} параметрі ВМ-дағы барлық осалдықтардың базалық бағаларын ескереді. Осалдықтардың әрбір базалық бағалары шабуылдаушының осы осалдықты пайдалану мүмкіндіктерінің дәрежесін ескереді. Сондай-ақ, шабуылдаушы келтіруі мүмкін зиян өлшемін ескеруге болады. Базалық көрсеткіштердің экспоненциалды қосындысы осалдықтар санының негізінде олардың мәндерінің логарифмдік масштабтағы ауытқуларын бағалауға мүмкіндік береді.

Екінші жағынан, $A_{U_{VM}}$ ВМ-ның осалдығын бағалау шабуылдаушының виртуалдық машинаның осалдығын пайдалану қабілетін көрсетеді және пайдаланылған желілік қызметтер санының мүмкін болатын желілік қызметтердің жалпы санының қатынасына байланысты. FS_{VM} жоғары бағалауы - бұл осалдықтар үшін қаскүнемнің мақсатына жетудің бірнеше жолдары бар екенін білдіреді.

Осылайша, FS_{VM} функционалды тұрақтылық көрсеткіші ВБО-дағы әрбір виртуалдық машинаның функционалды тұрақтылығы мен киберқауіпсіздігі деңгейінің сандық бағалауын көрсетеді. FS_{VM} функционалды тұрақтылық көрсеткіші ВБО-дағы әрбір виртуалдық машинаның функционалды тұрақтылығы мен киберқауіпсіздігі деңгейін анықтау үшін пайдаланылуы мүмкін.

FS_{VM} аса жоғары мәні бар виртуалды машинаға компрометирленген виртуалдық машиналардан киберқатерді болдырмау үшін қорғаныс жағы киберқауіпсіздіктің тиімді құралдарын қолдану қажет. FS_{VM} мәнін азайту үшін шабуылдаушылардың виртуалдық бұлттық ортаға теріс әсерінің шамасына байланысты шабуылдың әсерін азайту стратегиялары негізделді.

Айта кетейік, қарсы шараларды таңдау – бұл кешенді мәселе, оған тек техникалық қарсы шаралар кіреді, мысалы:

– шабуылдың дереккөзі төбесімен сессияны аяқтау;

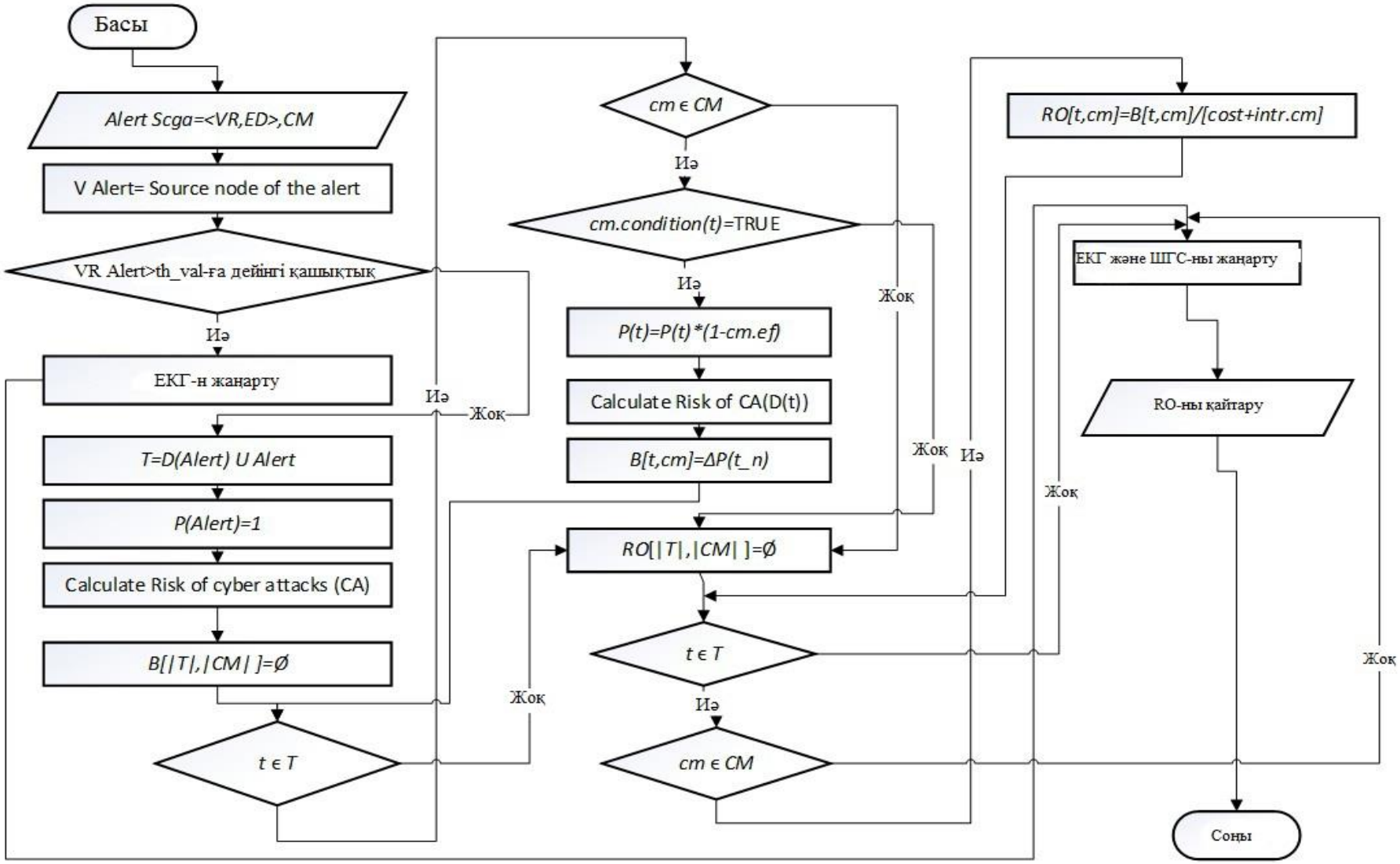
– пайдаланушыға хабарлама жіберу;

– желідегі серверге кіруді бұғаттау;

– IP-ді бұғаттау үшін қауіпсіздік сервистерінің конфигурациясын өзгерту, сонымен қатар техникалық құралдарды қаржыландыру бойынша ұтымды стратегияны таңдау. Ал мұндай стратегияны таңдау мәселесі тәуелсіз деп қарастырылады және оны шешуге біздің кейбір зерттеулеріміз [94, 95], сондай-ақ басқа авторлардың жұмыстары [96, 97] да арналған.

Алынған нәтижелер негізінде Probe типті шабуылды мысалға ала отырып, қарсы шаралар таңдау алгоритмі ұсынылды (сурет 13).

Алгоритм жұмысының мәні келесіден тұрады. Нақты кибершабуыл сценарийі үшін $(cm \in CM)$ қарсы шаралары таңдалады. Алгоритмнің жұмысы үшін кіріс деректері (*Alert*) желілік анализатордан, шабуылдар графынан,



Сурет 13 – ВБО-на Probe кибершабуылының әсерін азайту бойынша қарсы шараларды таңдау алгоритмі

сондай-ақ ықтимал қарсы шаралары бар деректер қорлары қатерлі хабарлама ($\{CM\}-$ ВБО-ды қорғауға арналған ықтимал қарсы шаралар бар жиын). Алгоритмнің жұмысы желілік анализатордан алынған қатер хабарламасына жауап беретін ХКГ-дағы төбені таңдаудан басталады. Осы қатерлердің хабарламасы үшін мақсатты төбеге дейінгі уақытша қашықтық есептеледі.

Егер алынған мән шекті мәннен (th_val) артық болса, онда cm қарсы шарасын таңдау жүргізілмейді. Әрі қарай ХКГ жаңартылады және жүйедегі қатер туралы жаңа хабарламаларды қадағалау жүргізіледі. Қарсы шараларды таңдаудың кешенді көрсеткішінің ең аз мәнін беретін қарсы шара сұранысқа сәйкес анықталады. Алгоритмнің жұмысы аяқталғанға дейін ШГ және ХКГ-нің сценарийлері жаңартылады.

Қарсы шараларды таңдау мақсатына жету үшін $CO.$ қарсы шараларды таңдаудың кешенді көрсеткіші қолданылады.

$$CO = \left(\left(h_1 \cdot JA\right) + \left(h_2 \cdot VA\right)\right) \Big/ k, \qquad (2.29)$$

мұнда $h_1, h_2 -$ ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздігіне қарсы шаралар көрсеткіштерінің әсер ету сипаттамалары;

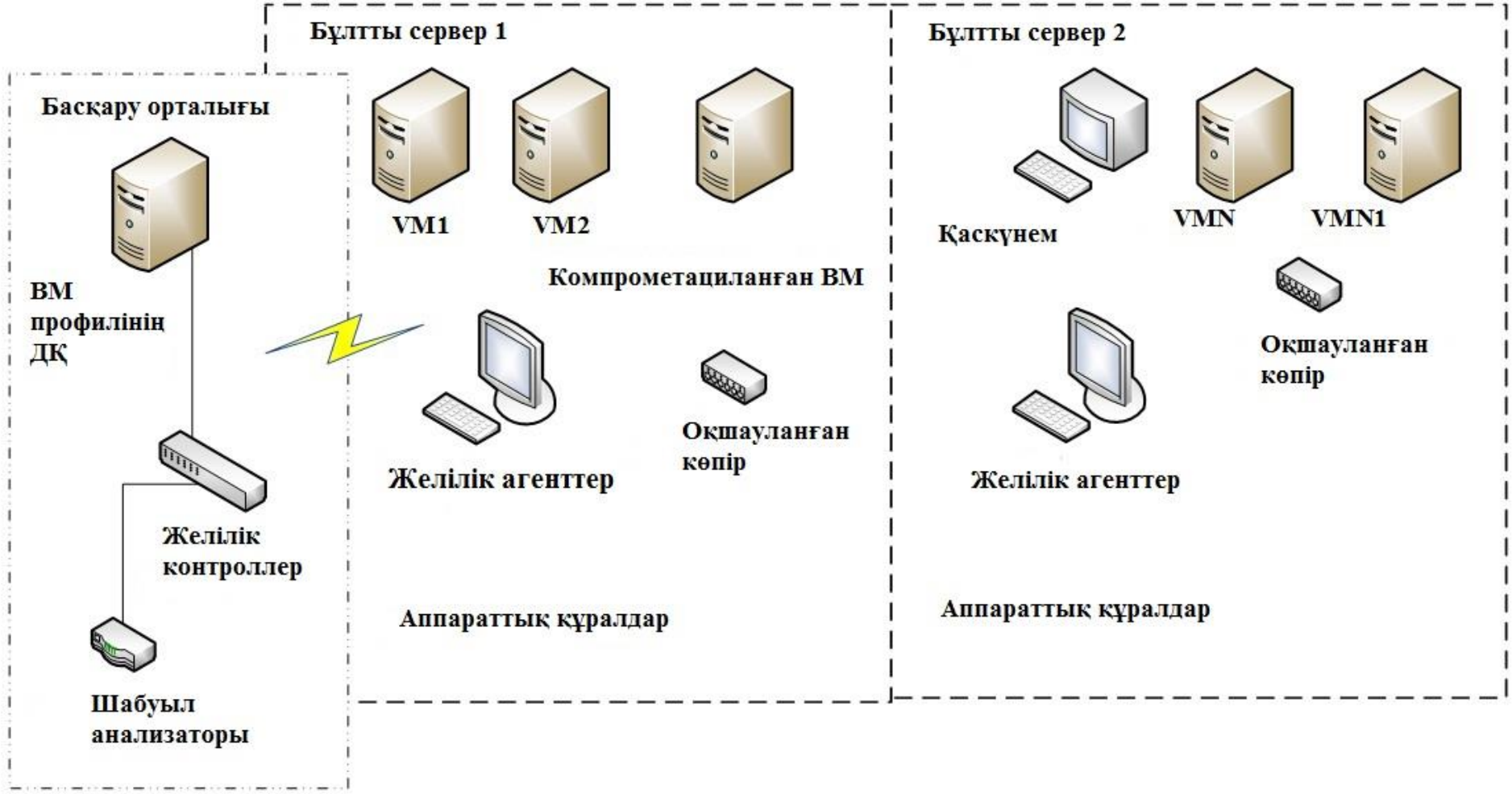
$JA-$ теріс әсердің шамасы, ол «Қызмет көрсету деңгейі туралы келісімге» ($Benefit\,(or\quad B)$) қатысты қарсы шараларды қолдану нәтижесінде туындайды; $VA-$ құн, ол ресурстар мен жедел күрделілік тұрғысынан қарсы шараларды қолдану үшін қажетті шығындарды көрсетеді (көрсеткіш жоғары болған сайын, (cost) - құны соғұрлым көп); $k-$ нормалау коэффициенті.

Зерттеу барысында бағдарламалық-конфигурацияланатын желі негізінде ВБО-ның функционалды тұрақтылығын қамтамасыз ету әдістемесі әзірленді. Әдістеме «Инфрақұрылым қызмет ретінде» қызметіне сүйене отырып әзірленді. Атап айтқанда, бұлттық қызметтерді пайдаланушылар кез келген операциялық жүйелерді немесе қосымшаларды орната алады. Бұл ретте келесі шектеу бар. Әдістемені қолдану хост негізіндегі басып кіруді анықтау жүйелерімен байланысты емес. Атап айтқанда, шабуылдарды анықтау үшін шифрланған трафикті қалай өңдеу керектігі шешілмейді. Әдістеме тек паравиртуализация негізіндегі жүйелерде ғана қолданылуы мүмкін [52-54, 92,93].

Әдістеменің шығыс деректері: шабуылдар графы, хабарламаларды корреляциялау графы, желілік анализатордан хабарлама, виртуалдық машиналардың профильдері. Бағдарламалық-конфигурацияланатын желі негізінде тестілік виртуалдық бұлттық ортасын тестілеудің функционалдық сұлбасы 14 -суретте көрсетілген.

Тестілік виртуалдық бұлттық орта келесідей элементтерді қамтиды: желілік агенттер, ВМ профильдерінің деректер қоры (ДҚ), желілік контроллер, шабуыл анализаторы және аппараттық құралдар, мысалы, коммутатор немесе маршрутизатор.

Желілік агент бұлттың әрбір серверінде орнатылады. Ол желілік көпірлер (bridge) арқылы өтетін трафикті сканерлеу үшін арналған.



Сурет 14 – Бағдарламалық-конфигурацияланатын желілер негізіндегі ВБО-ның функционалдық схемасы

Көпірлер физикалық бұлттық серверіндегі ВМ-лар арасындағы барлық трафикті бақылайды. ВМ профильдерінің деректер қоры әр машинаның күйі туралы ақпаратты қамтиды. Виртуалдық машиналар бұлттық ортада нақты ақпаратты алу үшін бейімделеді:

- ВМ күйін;
- қызмет күйі;
- ашық порттар күйлерін және т.б.

Бірнеше басқа машиналарға қосылған кез келген ВМ басымдылық болып табылады. Бұл көптеген байланыстары бар ВМ-дың компрометация әсері тұтастай алғанда ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздігінің айтарлықтай төмендеуін тудыруы мүмкін. Сонымен қатар, оған қатысты хабарламалардың дұрыстығын тексеру үшін ВМ-да жұмыс істейтін қызметтер туралы ақпаратты сақтау қажет. Қаскүнем желіні зерттеу үшін және кез келген ВМ-ға ашық порттарды іздеу үшін порттарды сканерлеу бағдарламасын пайдалана алады. Сондықтан ВМ-дағы кез келген ашық порт туралы ақпарат және ашық порттардың тарихы ВМ-дың осалдығын анықтауда маңызды рөл атқарады. Барлық осы факторлар жиынтығы ВМ-лар профилін құрайды. ВМ-дың профильдері деректер базасында сақталады және осалдықтар, желілік анализатордың хабарламалары, ашық порттар, сервистер және т.б. туралы ақпараттардан тұрады.

Желілік контроллер бағдарламалық қайта құру желісі бойынша мүмкіндіктерді қолдау үшін негізгі компонент. Ол openflow хаттамасы негізінде желілік қайта құру виртуалдық функциясын орындайды. Ұсынылған әдістемеде желілік контроллердегі openvswitch және openflow хаттамалары үшін біріктірілген басқару функциялары қолданылады. Бұл бұлттық жүйе үшін кешенді негізде трафикті сүзгілеу кезінде қауіпсіздік ережелерін орнатуға мүмкіндік береді. Желілік контроллер openflow ағымдағы желісі, желілер туралы ақпаратты жинайды және шабуыл графын құру үшін оны шабуыл анализаторына енгізуді қамтамасыз етеді. Топологияның өзгеруі туралы ақпарат автоматты түрде контроллерге жіберіледі, содан кейін шабуыл графын қалпына келтіру үшін қайта өңделеді. Желілік контроллер, сонымен қатар, шабуыл анализаторына сәйкес келетін қарсы шараларды қолдануына жауап береді. Шабуыл анализаторы бағдарламалық-конфигурацияланатын желілер негізінде ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету әдістемесінің негізгі функцияларын жүзеге асырады, ол ШСГ-н және ХКГ-н құру және жаңарту сияқты процедураларды қамтиды.

Ұсынылған әдістеме бағдарламалық-конфигурацияланатын желілер негізінде ВБО-ның функционалды тұрақтылығын қамтамасыз ету алгоритмінің блок-схемасы түрінде 15 - суретте көрсетілген. Әдістеменің негізгі кезеңдерін келесідей сипаттауға болады. Бағдарламалық-конфигурацияланатын желілер негізінде ВБО-ның функционалды тұрақтылығын қамтамасыз ету әдістемесінің кезеңдері:

1 кезең. Қатер туралы хабарлама аламыз.

Қабылданған қысқартулар: ЖА – желілік анализатор,
ХКГ – хабарламаларды корреляциялау графы

Сурет 15 – Бағдарламалық-конфигурацияланатын желілер негізінде ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету алгоритмі

2 кезең. Бұл хабарламаны жүйедегі бұрыннан белгілі қатерлермен салыстырамыз.

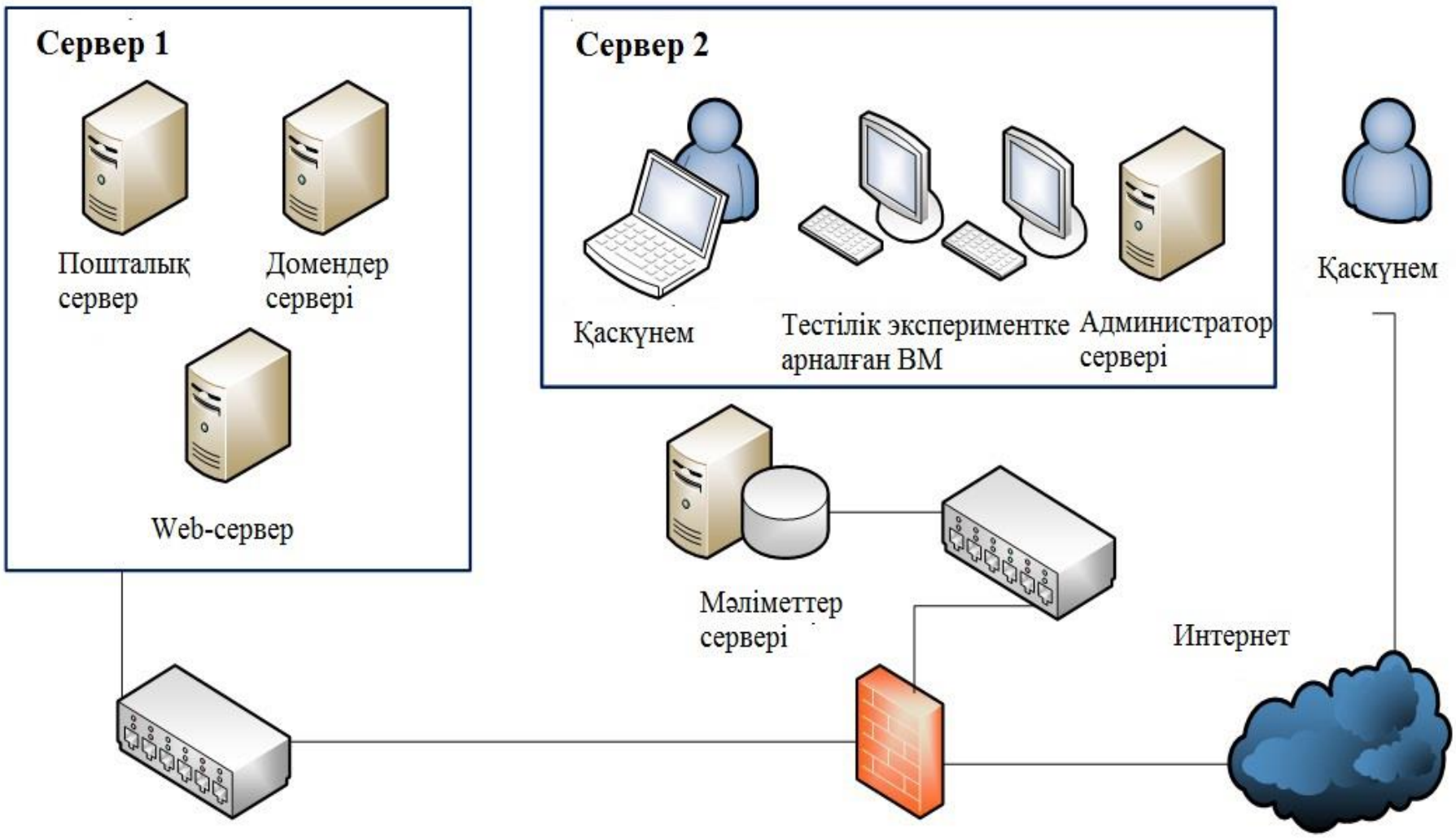
3 кезең. Хабарлама корреляциясынан өткіземіз. ВМ-дың функционалды тұрақтылық көрсеткішін есептеу және корреляция графын жаңартуды орындаймыз.

4 кезең. Қарсы шараларды таңдаудың кешенді көрсеткішінің мәні негізінде қарсы шаралар таңдаймыз.

5 кезең. Желілік контроллерге таңдалған қарсы шара бойынша деректерді жібереміз.

Алынған әдістер мен модельдерді тексеру мақсатында бағдарламалық-конфигурацияланатын желілер негізінде ВБО-ның функционалды тұрақтылығын қамтамасыз ету бойынша тәжірибелік зерттеулер жүргізілді. Алынған ғылыми нәтижелердің тиімділігін бағалау үшін 25 виртуалдық машинаны қамтитын тестілік виртуалдық бұлттық орта әзірленді. 16 – суретте тестілік орнының құрылымдық схемасы көрсетілген.

Мысалы, физикалық немесе виртуалдық коммутаторды орнату кезінде Open vSwitch-ті пайдаланғанда, оны пакеттерді әртүрлі жолдармен жіберу арқылы тестілеу қажет. Мысал ретінде, ping және tcpdump утилиталарын қарастыруға болады. Виртуалдық коммутатор үшін оны орындау қиын, өйткені виртуалдық коммутатор операциялық жүйе үшін көрінбейді. Алайда, ол тестілеу үшін арнайы құралдар жиынтығынан құралған.



Сурет 16 – Эксперименттік зерттеулер жүргізуге арналған стенд схемасы

Мысалы, коммутаторға келген пакетті тексеру үшін команданы орындау

$ ovs-appctl ofproto/trace br0 in_port=2,vlan_tci=5

егер пакет дұрыс болмаса, осындай нәтиже аламыз

Bridge:br0Flow:in_port=2,vlan_tci=0x0005,dl_src=00:00:00:00:00:00,dl_dst=00:00:00:00:00:00,dl_type=0x0000

Rule: table=0 cookie=0 priority=0 OpenFlow actions=resubmit(,1) Resubmitted flow:in_port=2,vlan_tci=0x0005,dl_src=00:00:00:00:00:00,dl_dst=00:00:00:00:00:00,dl_type=0x0000

Resubmitted regs: reg0=0x0 reg1=0x0 reg2=0x0 reg3=0x0 reg4=0x0 reg5=0x0 reg6=0x0 reg7=0x0 reg8=0x0 reg9=0x0 reg10=0x0 reg11=0x0 reg12=0x0 reg13=0x0 reg14=0x0 reg15=0x0 Resubmitted odp: drop

Resubmitted megaflow: recirc_id=0,in_port=2,vlan_tci=0x0005,dl_src=00:00:00:00:00:00/01:00:00:00:00:00,dl_dst=00:00:00:00:00:00/ff:ff:ff:ff:ff:f0,dl_type=0x0000

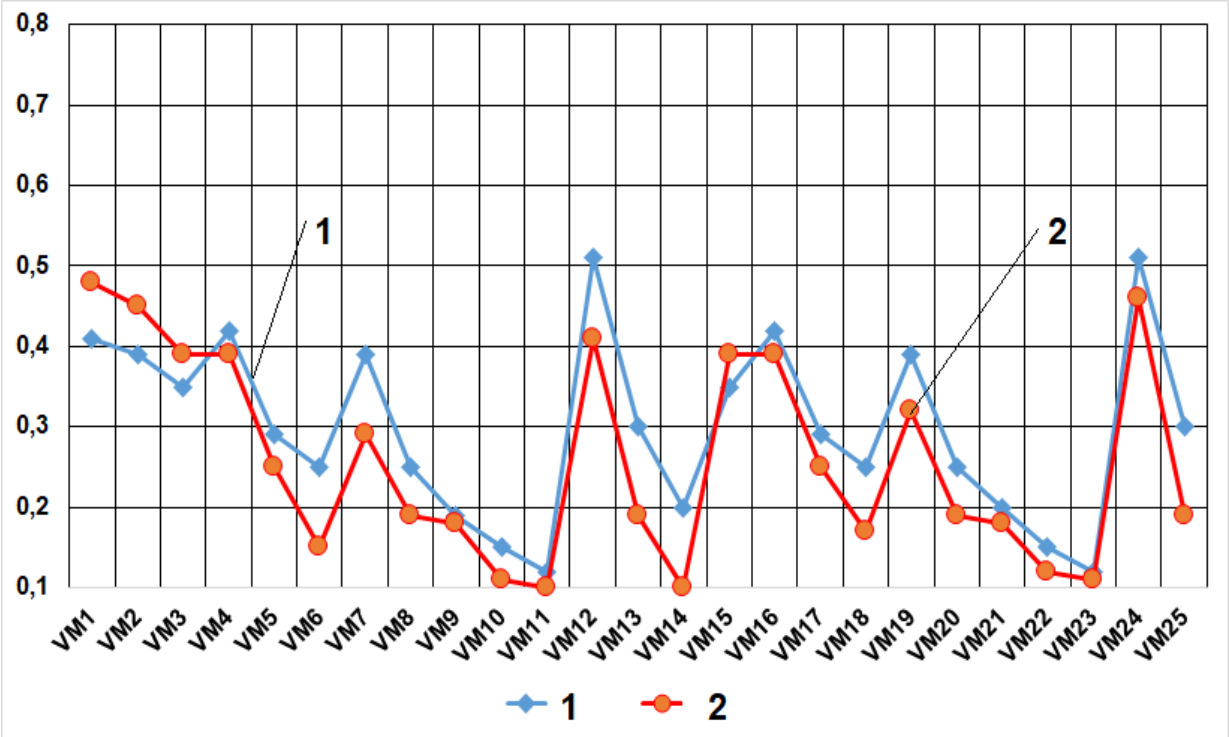
Rule: table=1 cookie=0 priority=0 OpenFlow actions=drop Final flow: unchanged Megaflow: recirc_id=0,in_port=2,vlan_tci=0x0005,dl_src=00:00:00:00:00:00/01:00:00:00:00:00,dl_dst=00:00:00:00:00:00/ff:ff:ff:ff:ff:f0,dl_type=0x0000 Datapath actions: drop

Ұсынылған әдістеме мен математикалық модельдерді эксперименттік тексеру кезінде алынған негізгі нәтижелер 17–20 - суреттерде келтірілген.

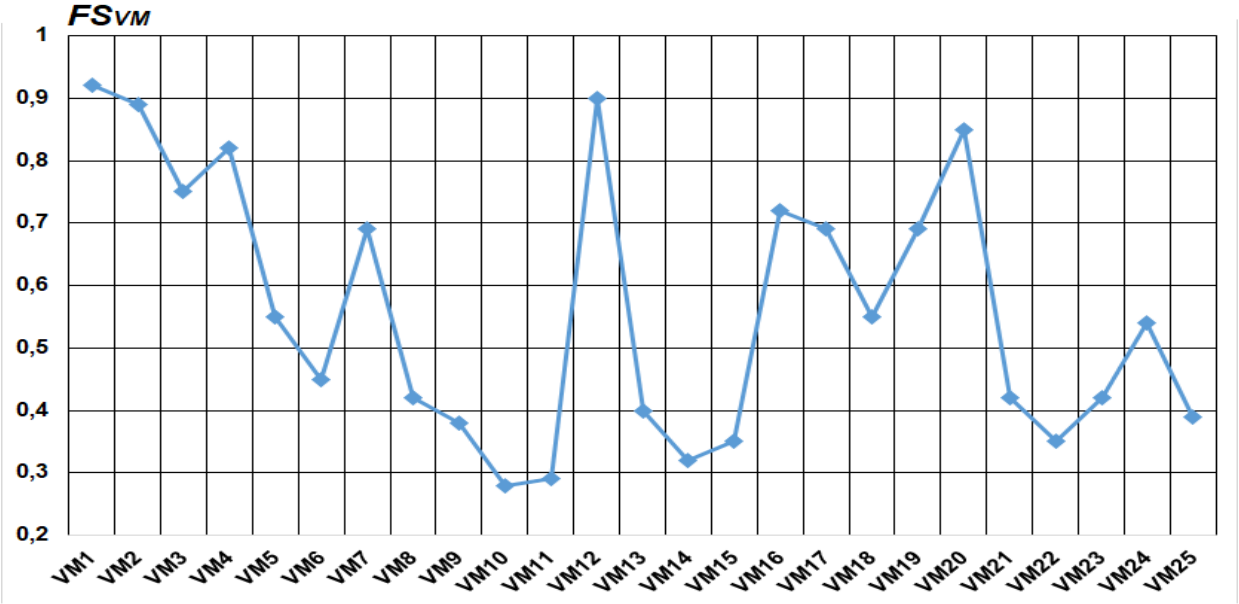
17–суретте $A_{U_{VM}}$ – ВБО-дағы виртуалдық машинаның (ВМ) осалдығын қолданғандағы бағалау(1 сызық) және A_{VM} –виртуалдық машина осалдығын бағалаудың (2 сызық) графиктері көрсетілген. Бұл көрсеткіштер (2.27) - (2.28) формулаларын қолдана отырып, эксперимент деректерін өңдеу нәтижесінде алынды.

17–суреттегі графикте виртуалдық машиналардағы осалдықтарды қаскүнем оларды компрометациясы үшін қаншалықты қолдана алатындығын көрсетеді. Бұл көрсеткіштер неғұрлым төмен болса, қаскүнемдер өз мақсатына жету тәуекелі соғұрлым аз болатынын ескереміз. Егер көрсеткіштердің бірі 0,5 мәннен асып кетсе, онда ықтималдылықтың жоғары үлесімен ВБО-ның функционалды тұрақтылығының жалпы көрсеткіші де жоғары болады деп есептеуге болады. Бұл өз кезегінде, виртуалдық машиналар компрометациясының ықтималдығы жоғары екендігін және оған сәйкес қарсы шаралар қабылданатынын білдіреді.

Функционалды тұрақтылық (FS_{VM}) көрсеткішіне байланысты ВМ-ны бағалау 18–суретте көрсетілген. Сурет тестілік виртуалдық бұлттық ортасының немесе нақты ақпараттандыру нысаны үшін функционалды тұрақтылығының жалпы күйін көрсетеді. FS_{VM} мәні неғұрлым төмен болса, жеке бұлттық ортада виртуалдық машинаның функционалды тұрақтылығының күйі соғұрлым жоғары.



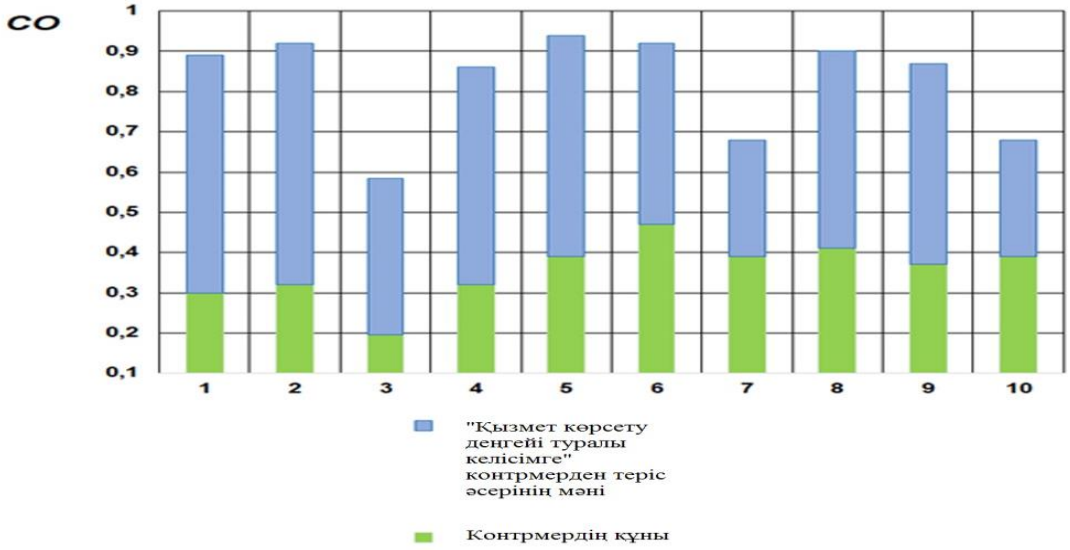
Сурет 17 – ВМ-ды $A_{U_{VM}}$ (1 сызық) және A_{VM} (2 сызық) көрсеткіштер тұрғысынан бағалау графигі



Сурет 18 – FS_{VM} көрсеткіші тұрғысынан ВМ-ны бағалау графигі

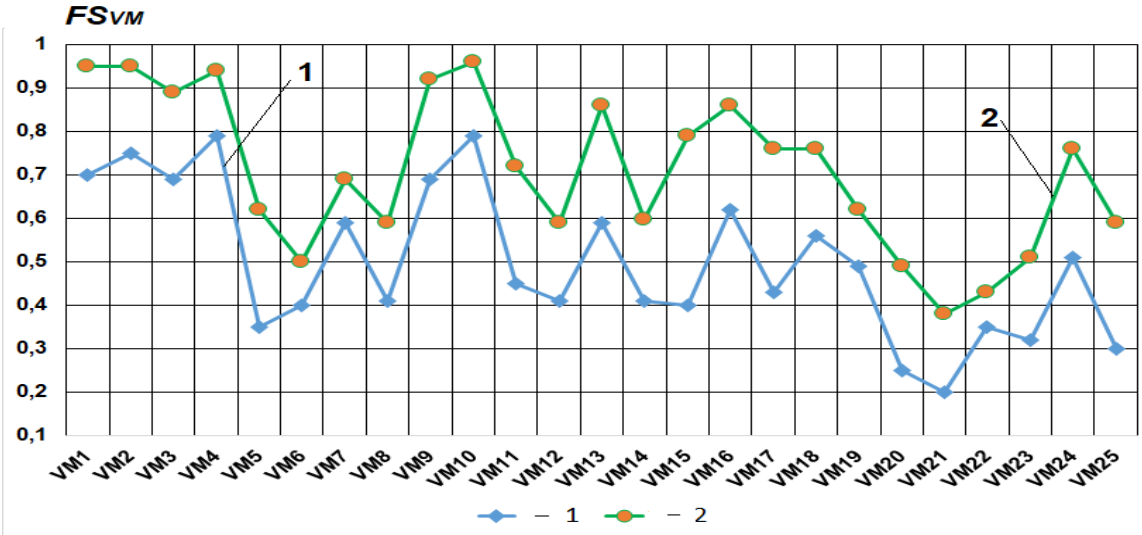
19–суретте *CO* қарсы шараларды таңдаудың кешенді көрсеткіші үшін графиктер көрсетілген, ол « SLA қызмет көрсету деңгейі туралы келісім» қарсы шараларды теріс әсер мәнін көрсетеді. Алынған график, сонымен қатар, ресурстар мен жедел күрделілік тұрғысынан қарсы шараны қолдану үшін қажет

шығындарды көрсетеді (көрсеткіш неғұрлым жоғары болса, құны (cost) соғұрлым көп болады). Бұл көрсеткіштер *CO* қарсы шараларды таңдаудың кешенді көрсеткішін бірге көрсетеді. Айта кету керек, *CO* қарсы шараларын таңдаудың жоғары кешенді көрсеткіші бар қарсы шаралар виртуалдық бұлттық ортаның барлық инфрақұрылымын айтарлықтай өзгерте алатын аса маңызды және сирек пайдаланылатын қарсы шараларға сәйкес келеді.



Сурет 19 – ВБО-сы үшін *CO* қарсы шараларны таңдаудың кешенді көрсеткішінің диаграммасы

20–суретте сәйкес қарсы шараларды қолданғанға дейін және кейін тестілік виртуалдық машиналар үшін FS_{VM} виртуалдық машина көрсеткішінің мәндері келтірілген.



(1 сызық– қарсы шараларды қолданғаннан кейін, 2 сызық–қарсы шараларды қолданғанға дейін)

Сурет 20 – ВМ үшін FS_{VM} көрсеткішін өзгерту

Бұл суретте графикті талдау виртуалдық машиналардың осалдығын FS_{VM} -ден төмендетудің орташа көрсеткіші шамамен 12-17% құрайды. Бұл бағдарламалық-конфигурацияланатын желілер негізінде ВБО-ның тиімділігін арттыруға мүмкіндік береді.

Осылайша, жүргізілген зерттеулердің жаңалығы модельдер жетілдірілді:

– ВБР-на шабуылдардың әсері. Ұсынылған модель қолданыстағылардан айырмашылығы, бұл хабарламалардың корреляциялау графында қабырғаларды құру үшін жүйедегі көршілес төбелерден хабарламалардың түсімдерінің арасындағы уақыт айырмашылығын ескеретін функция қолданылған;

– ВБР күйін бағалау. Модель қолданыстағылардан айырмашылығы, бұл қарсы шараларды таңдау үшін ВБР-на қызмет көрсету деңгейі туралы келісіміне қарсы шаралардың әсерін бағалау көрсеткіші және ресурстар мен жедел күрделілік тұрғысынан қарсы шараны қолдану үшін қажетті шығындар көрсеткіші қолданылады;

– бағдарламалық-конфигурацияланатын желілер негізінде ВБО-ның функционалды тұрақтылығын қамтамасыз ету әдістемесі ұсынылды. Бұл әдістеме, белгілі әдістемелерге қарағанда, виртуалдық желілерді қайта конфигурациялау және шабуылдарды анықтау механизміне негізделген, бұл виртуалдық машиналардың компрометацияға функционалды тұрақтылығын арттыруға мүмкіндік береді. Ол үшін FS_{VM} кешенді көрсеткіші қолданылады.

Екінші тарау бойынша қорытындылар

Диссертацияның екінші тарауында келесі нәтижелер алынды:

– ақпараттық желілер мен қашықтықтан оқыту жүйелеріне шабуыл жасау қаупін сипаттайтын көрсеткіштер үшін, оны интерпретациялау контекстінде ақпаратты қорғау жүйелерін сипаттау бойынша мәселені шешу моделі алынды. Ақпараттық желілер мен қашықтықтан оқыту жүйелеріне шабуыл жасау қатерлерінің нақты қисынды марковтық модельдерін құруға болады;

– ҚОЖ-нің киберқауіпсіздігін инвестициялаудың ұтымды стратегиясын таңдау модельдері мен алгоритмдері жиынтығымен ҚОЖ-н киберқорғалған және функционалды тұрақтылығын құру әдіснамасын жетілдіруге болатындығы көрсетілген;

– ақпараттық желіде және қашықтықтан оқыту жүйесінде киберқатерді анықтау әдісі жетілдірілді. Жетілдірілген әдіс, қолданыстағы әдістерден айырмашылығы бөлінген желілік өзін-өзі оқыту рекурсивті алгоритмдерін және киберқатерлер түріне байланысты қарсы шараларды таңдауды (атап айтқанда, қашықтықтан оқыту жүйесінің ақпараттық желісін қорғау тараптары үшін қаржылық немесе техникалық стратегияларды) қамтиды;

– киберқатерді анықтау әдістеріне ұсынылған толықтыруларды жүзеге асыру қашықтықтан оқыту жүйесінің ақпараттық желілерінің қорғалу дәрежесін

жақсарту үшін қажетті қарсы шаралар туралы негізделген шешімдерді шығаруды жүзеге асыруға мүмкіндік беретіні көрсетілген. Бұл ретте қашықтықтан оқыту жүйесінің ақпараттық желілерін басқару мақсаттарының динамикалық өзгеруі жағдайында киберқатерлер туралы ақпарат нақты уақытта қашықтықтан оқытудың ақпараттық желілік жүйесінде әр түрлі дереккөздерден келіп түсетіні талданды;

– ҚОЖ-нің бағдарламалық-конфигурацияланатын желілері үшін ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету үшін математикалық модельдер жетілдірілді. Модель кибершабуыл параметрлерінің ВБР-на әсерін ескере отырып жетілдірілді. Сондай-ақ модельде ВБР-дың күйін және бағдарламалық-конфигурацияланатын желілер үшін кешенді көрсеткіш негізінде мүмкін болатын қарсы шараларды таңдау ескеріледі. Виртуалдық бұлттық ортаға шабуыл графы әзірленді, ол жүйенің барлық белгілі осалдықтары туралы ақпарат алуға мүмкіндік береді, сонымен қатар ВБР-ның функционалды тұрақтылығы мен киберқауіпсіздігінің күйін нақты уақыт режимінде көрсетеді. ҚОЖ-нің ақпараттық қауіпсіздік администраторына ұсынылған модельдерді кешенді қолдану нәтижесінде ықтимал киберқатер мен шабуылдарды, атап айтқанда, ҚОЖ-нің виртуалдық бұлттық желісінде анықталған оқиғаларды корреляциялау есебінен болжауға болады;

– бұлттық ортадағы қатерлерді талдау үшін алгоритмдер әзірленді, бұл жұмыстың нәтижесінде виртуалдық бұлттық ортасына шабуыл жасаудың бір немесе бірнеше жолын алу; қарсы шара таңдау, оның нәтижесі ҚОЖ-не және оның ВБР-на шабуылдың нақты сценарийі үшін қарсы шараларды таңдау;

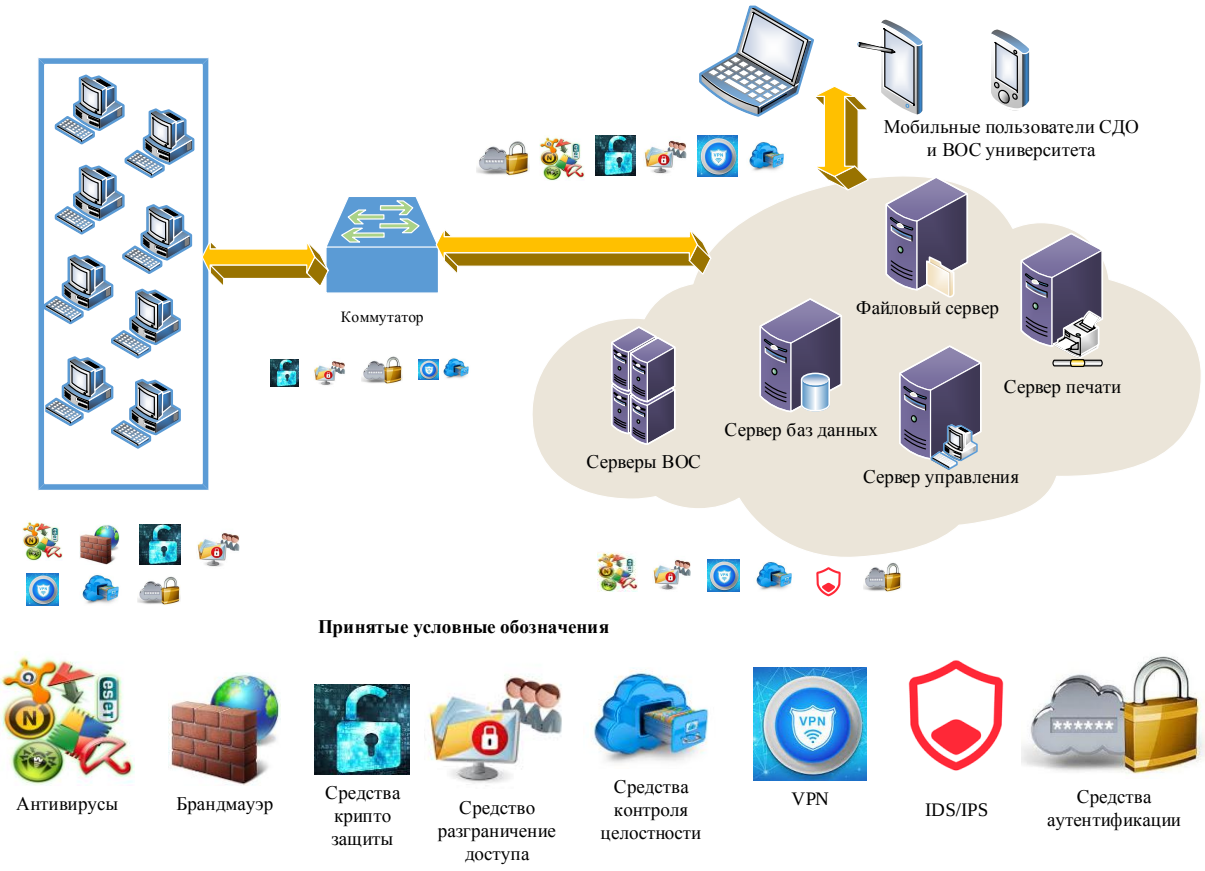
– бағдарламалық-конфигурацияланатын желілерді қолдану негізінде ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету әдістемесі ұсынылды. Бұл әдістеме ҚОЖ-нің виртуалдық желілерін қайта конфигурациялау және кибершабуылдарды анықтау негізінде виртуалдық машиналардың компрометациясының тұрақтылығын арттыруға бағытталған;

– әзірленген әдістеме мен модельдерге эксперименталды апробация жүргізілді. Алынған нәтижелердің адекватылығын растау үшін тестілік виртуалдық бұлттық орта жүзеге асырылды. Ұсынылған шешімдер жалпы алғанда ҚОЖ-н және ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздік көрсеткішін белгілі шешімдермен салыстырғанда 12-17%-ға арттыруға мүмкіндік беретіні эксперименталды көрсетілді.

3 ЖАППАЙ ҚЫЗМЕТ КӨРСЕТУ ЖҮЙЕСІ РЕТІНДЕ ҚАШЫҚТЫҚТАН ОҚЫТУ ЖҮЙЕСІНІҢ КИБЕРҚАУІПСІЗДІГІН БАСҚАРУ ТӘСІЛДЕРІН ҚАЛЫПТАСТЫРУ ӘДІСТЕМЕСІ

3.1 Ақпараттық қауіпсіздікті басқару жүйесін құру және ақпаратты қорғау құралдарын орналастыру нұсқаларын таңдау процесінде жаппай қызмет көрсету жүйесі ретінде қашықтықтан оқыту жүйелерін компьютерлік модельдеу

Қазіргі ҚОЖ-н және олардың ақпараттық қауіпсіздікті басқару жүйелерін (АҚБЖ) техникалық сипаттамалар мен архитектуралардың жиынтығы бойынша жаппай қызмет көрсету жүйесі (ЖҚКЖ) ретінде сипаттауға болады. ЖҚКЖ-нің барлық ықтимал схемалары, атап айтқанда, шығындармен, күтумен, шектеулі сыйымдылық жинақтауышымен және т.б., ол ҚОЖ-мен аралас басымдылықтары бар және өтінімдердің кезекте болуының шектеусіз уақытымен жүйелерді ұсынады. Бүгінгі күні ҚОЖ – бұл клиент-сервер архитектурасына сәйкес келетін күрделі ақпараттық жүйелер (АЖ) (сурет 21).



Сурет 21 – Қашықтықтан оқыту жүйесінің ақпараттық желісі мен виртуалдық бұлттық ортасының құрылымы

ҚОЖ-лері келесі негізгі элементтерді қамтиды: ҚО сервері(лері); деректер базасын; модульдер мен ішкі жүйелер: 1) басқару; 2) білім беру ақпаратын жеткізу; 3) тест тапсырмаларын генерациялау; 4) басқару және т.б.

Қашықтықтан оқыту жүйелерін пайдаланудың нақты тәжірибесінде транзакцияның дамыған механизімімен оқушылардан және ПОҚ-нан сұраныс кезегі қалыптасады. Абоненттердің (ҚОЖ пайдаланушыларының) санының ұлғаюына және/немесе оған сұраныстардың артуына қарай (әдеттегі DoS/DDoS шабуылдар нәтижесінде ұйымдастыруға болады) кезекте дағдарыстар туындауы мүмкін. Атап айтқанда, сұраныстар қызмет көрсетілгеннен тезірек жинақталады. Қашықтықтан оқыту жүйесінде арнайы клиенттер бар екенін ескереміз. Арнайы клиенттерге, мысалы, қашықтықтан оқыту жүйесінің администраторлары немесе жоғары басымдыққа ие қызмет ететін ЖОО басшыларын жатқызуға болады. Мысалы, R2L және U2R класының шабуылдары салдарынан басымдылық жасанды түрде өзгеруі мүмкін. Аталған жағдайлар ҚОЖ-н кибершабуылдардан қорғаудың қажетті механизмдерін талдау және таңдау мәселесін айтарлықтай күрделендіре алады [99].

Практикада қашықтықтан оқыту жүйесіндегі кибершабуылдармен байланысты проблемаларды шешудің әртүрлі нұсқалары қолданылады. Ең көп таралған нұсқа - неғұрлым қуатты серверді пайдалану, қауіпсіз операциялық жүйелерге ауысу, мысалы, Linux. ҚОЖ-нің қорғау жүйесін құрудың оңтайлы нұсқасын таңдау үшін әртүрлі жағдайларды модельдеу қажет. Абоненттерден жаңа сұраныстардың пайда болуы; ҚОЖ-дегі транзакциялардың ұзақтығы; ҚОЖ-де осалдықтар туындайтын қарқындылық; ҚОЖ-де осалдықтар анықталатын қарқындылық; ҚОЖ-де анықталған осалдықтарды ҚОЖ-дегі қызметкерлер немесе бағдарламалық қамтамасыз ету әзірлеушісімен жойылатын қарқындылық (2-тарауды қараңыз), бұл әртүрлі бөлу заңдарымен сипатталады. Демек, бұл фактіні ЖОО-ның шектеулі бюджеті жағдайында ақпаратты қорғау құралдарын таңдаудың оңтайландырылған мәселелерін шешу кезінде қабылдау қажет. Бұл жағдайда ҚОЖ-нің топологияларының әртүрлі нұсқалары, демек, ҚОЖ-і үшін киберқауіпсіздікті және ақпаратты қорғаудың құралдарын оңтайлы таңдау бойынша әртүрлі есептер қойылуы мүмкін.

Жалпы буферлік жадысы бар аралас басымдылықтары бар көп арналы ЖҚКЖ-нің топологиялық схемасы 22–суретте көрсетілген.

22–суретте көрсетілген схема келесідей жұмыс істейді. Талаптар (қызмет көрсетуге өтінімдер, мысалы, дәріс, зертханалық жұмыс немесе пән шеңберінде тесттер ашу) ҚОЖ-нің серверіне немесе ВБО-на түседі. Сервер, негізгі басқару құрылғысы ретінде, ҚОЖ-нің администраторы орнатқан сәйкесінше бағдарлама мен басымдылықтардың көмегімен абоненттерді ауыстыру блогын қамтиды, атап айтқанда жүйеде тіркелген білім алушыларды немесе қонақтық қолжетімділікті ашады. Ең жоғарғы басымдылық ҚОЖ-де және АҚБЖ-дегі әртүрлі саясат негізінде берілуі мүмкін. Мысалы, ең жоғарғы басымдылық курс модераторына,

деканға, кафедра меңгерушісіне немесе қашықтықтан оқыту жүйесінің администраторына берілуі мүмкін. Немесе басымдылық тестті, зертханалық жұмыс және т.б. мерзімінен бұрын орындау принципіне сүйене отырып берілуі мүмкін.

Сурет 22 – ЖҚКЖ ретіндеҚОЖ-нің функционалды жүйесі

Ақпараттық қауіпсіздік пен киберқауіпсіздікті қамтамасыз ету үшін әлемнің жетекші ЖОО АҚБЖ-н енгізуде. Мұндай АҚБЖ, әдетте, ISO/IEC 27k стандарттары талаптарының негізінде құрылады. Айта кету керек, қолданыстағы стандарттарда белгілі бір ұйымға, мысалы, ЖОО-на қатысты АҚБЖ-не қойылатын жобалық талаптарды бірегей қалыптастыруға мүмкіндік беретін нақты әдістемелер жоқ екенін атап өткен жөн. Онда қандай да бір бизнес процесті қорғау үшін енгізу қажет, мысалы, ҚОЖ-н немесе бүкіл ұйым үшін ақпараттық қауіпсіздік саясатына (АҚС) қатысты ақпараттық қауіпсіздіктің әртүрлі аспектілері туралы сөз болып отыр. Бұл жағдайда ақпараттық қауіпсіздікті қамтамасыз ету басымдылықтарын таңдау және АҚБЖ-н функционалды қолдану үшін оның функционалдық ерекшеліктерін сипаттайтын формальды модель болуы қажет.

Мұндай модельдің параметрлерін зерттеу ЖОО-ның цифрлық білім беру ортасының немесе ҚОЖ-нің киберқауіпсіздігі мен ақпараттық қауіпсіздігінің қандай аспектілеріне басымдылық берілуі керектігін түсінуге мүмкіндік береді. Өз кезегінде, АҚБЖ-нің формальды моделінің құрылымын түсіну үшін ҚОЖ-нің АҚБЖ-н зерттеу барысында формальды әдістердің қайсысы көбірек қолданылатынын ескеру қажет. Егер ұқсастықты анықтау мүмкін болса, онда ISO/IEC 27k стандарттарымен регламенттелетін жобалаудың формальды әдістемелері жалпы ЖОО-ның цифрлық білім беру ортасы және ҚОЖ үшін АҚБЖ-н құру мәселелеріне бейімдеуге болады деп болжауға болады.

Ұйымның, мысалы, ЖОО-ның АҚБЖ-н қарастырайық. [100] сәйкес АҚБЖ – бұл «ұйымды басқарудың жалпы жүйесінің бір бөлігі және ол ақпараттық ресурстар үшін тәуекелдерді бағалауға негізделеді». АҚБЖ ұйым үшін ақпараттық қауіпсіздік пен киберқауіпсіздіктің жаңа мәселелеріне қарай жобалайды, құралады, пайдаланады, мониторингті жүзеге асырады, қайта қарайды, сүйемелдейді және жетілдіреді. Мұндай анықтама ақпараттық қауіпсіздіктің типтік мәселелерін бірнеше рет шешуге арналған жүйе класын түсіндіру ретінде АҚБЖ туралы айтуға негіз береді. Сонымен қатар, АҚБЖ-і мен ЖҚКЖ-і арасындағы ұқсастықтар айқын.

Олардың арасындағы ұқсастықтарды анықтау мақсатында ЖҚКЖ мен ҚОЖ-нің АҚБЖ-нің қызмет көрсету процедураларының (ҚКП) сипаттамаларын салыстыру нәтижелері 3–кестеде келтірілген.

3–кестеде ЖҚКЖ мен ҚОЖ-нің АҚБЖ-нің қызмет көрсету механизмдерінің толық сәйкес келуі көрінеді. Бұл, өз кезегінде, осы екі типті жүйелердің қызмет көрсету процедураларының сәйкес сипаттамаларының сәйкестігін табуға мүмкіндік береді. Толық сәйкестікті көрсетеді және ҚОЖ-нің АҚБЖ мен ЖҚКЖ-де қызмет көрсететін жүйелердің құрылымында көрсетеді, бірақ оларда бірнеше әр түрлі жұмыс әдістері қолданылады. Бұдан басқа, өтінімдерге қызмет көрсету уақыты (ҚОЖ-н қорғаныс контурын жеңумен байланысты кибернетикалық тәуекелдерді өңдеу) өтінімдердің сипатына немесе клиенттердің талаптарына байланысты. Мұндай талаптарға, мысалы, кибернетикалық тәуекелдің (КрТ) максималды мәнін; кибернетикалық тәуекелді талдау және өңдеу бойынша іс-шараларды жүргізу үшін қажетті уақыт; ұйымның қызмет көрсететін жүйелерінің күйі мен мүмкіндіктерді (жалпы ЖОО-ның киберқауіпсіздік немесе ақпараттық қауіпсіздік бөлімшелері немесе ҚОЖ-нің киберқауіпсіздік бойынша жеке маманы) жатқызуға болады. Кейбір жағдайларда, сонымен қатар, қызмет көрсететін каналдардың істен шығу ықтималдығының параметрлерін ескеру қажет болуы мүмкін, мысалы, кейбір шектеулі уақыт аралығы аяқталғаннан кейін. ЖҚКЖ-нің бұл сипаттамасы барлық басқа өтінімдердің алдында басымдылыққа ие, себебі оны істен шығу ағыны ретінде модельдеуге болады. Дәл осындай дәлелдер ақпараттық қауіпсіздікті басқару жүйесі үшін де қолайлы [101].

ЖҚКЖ-нің құрылымын және оның функционалдық моделін жете талдау негізінде зерттеу барысында ЖҚКЖ-і мен ҚОЖ-нің АҚБЖ-і арасында құрылымдық-функционалдық ұқсастық орнатылды. Атап айтқанда, осы жүйелердің негізгі элементтерін жаппай қызмет көрсету теориясының (ЖҚКТ) АҚБЖ контекстінде ЖҚКЖ-нің (қызмет көрсету механизмі, қызмет көрсету жүйесінің құрылымы, қызмет көрсету процедурасының сипаттамалары) негізгі сипаттамалары түсіндірмелерінің мүмкіндігін қарастыру олардың толық сәйкес келетіндігін анықтады. Жүйенің ұқсастығы ҚОЖ-нің АҚБЖ-ін жобалау кезінде ЖҚКЖ-не тән математикалық аппараттарды және белгілі есептеу әдістерін пайдалануға мүмкіндік береді [102].

Кесте 3 – ЖҚКЖ-і мен ҚОЖ-нің АҚБЖ-нің қызмет көрсету механизмінің сипаттамаларын салыстыру

п/п	Жүйенің механизмінің сипаттамасы, қызмет көрсету процедуралары және құрылымы	ЖҚКЖ	ҚОЖ-нің АҚБЖ	Қорытынды
1	Қызмет көрсету механизмі анықталады:	Жүйенің қызмет көрсету процедураларының және қызмет көрсету құрылым сипаттамалары	ақпараттық қауіпсіздік тәуекелдерін өңдеуге арналған іс-қимылдардың реттілігін және ақпараттық қауіпсіздік бөлімшесінің құрылымын сипаттайтын ұйымның стандартымен (ереже, нұсқаулық)	Сәйкес (С)
2	Қызмет көрсету процедуралары	Қызмет көрсетушілер саны (N)	ҚОЖ үшін ақпараттық қауіпсіздік тәуекелдерін өңдеуге қатысатын талдаушылар саны	(С)
		Қызмет көрсету процедурасының ұзақтығы	Ақпараттық қауіпсіздіктің жеке тәуекелін өңдеу ұзақтығы	(С)
		Өтінімдер әрбір процедураларды орындау нәтижесінде қанағаттандырылады (топтық өтінімдер үшін)	Өтінімдер дискретті түрде түседі (тәуекелдер туралы ақпарат кезекпен келіп түседі)	АҚБЖ-де топтық өтінімдер жоқ
		Қызмет көрсететін каналдың істен шығу ықтималдығы	Қызмет көрсететін каналдың істен шығу ықтималдығы	(С)
3	Қызмет көрсету құрылымы жұмыс әдістерімен сипатталады:	тізбектелген, параллельді, аралас	тізбектелген, параллельді, аралас, сондай-ақ, қосымша ресурстарды тарту мүмкіндігі бар	(С)

Мысалы, ҚОЖ АҚБЖ-нің жобалық сипаттамаларын анықтау мақсатында одан әрі зерттеу үшін ЖҚКЖ-нің дифференциалдық теңдеулері қолданылады. АҚБЖ-де кезекте бір тәуекелден артық болмауы тиіс, мысалы, DoS/DDoS шабуылды жүзеге асыру тәуекелін қарастырайық.

ҚОЖ АҚБЖ-нің күйін S_i ретінде белгілейміз, бұл кезде АҚБЖ-нің енгізу кезінде өңделетін i $(i = 0,1,2,...)$ қатерлер кезегі бар. АҚБЖ-не кіруде t уақытында i тәуекелдің кезегі болу ықтималдығын $p_i(t)$ деп белгілейміз. Басқаша айтқанда, $p_i(t)$ - бұл АҚБЖ S_i күйде болу ықтималдығы. i-ші тәуекелдің кезегі бар ҚОЖ-нің АҚБЖ үшін тәуекелдер ағынының қарқындылығы және тәуекелдерді өңдеу қарқындылығы кезектің ұзындығына, атап айтқанда сәйкесінше $\lambda = \lambda_i$ және $\mu = \mu_i$, байланысты деп есептейміз.

$\Delta p_i(t)$ ықтималдықтың өзгеруінің моделін Δt уақыт аралығында тікелей t сәтте құру қажет.

Онда дифференциалдық теңдеулердің сәйкес жұбы келесідей болады [102, 103]:

$$\frac{dp_0(t)}{dt} = -\lambda_0 * p_0(t) + \mu_1 * p_1(t), \quad (3.1)$$

$$\frac{dp_1(t)}{dt} = \lambda_0 * p_0(t) - \mu_1 * p_1(t). \quad (3.2)$$

Егер осы екі теңдеуді толық ықтималдық қатынасымен толықтырсақ:

$$p_0(t) + p_1(t) = 1, \quad (3.3)$$

онда жоғарыда келтірілген үш қатынас қызмет көрсетуден бас тартумен бір каналды ЖҚКЖ күйінің ықтималдығы үшін Колмогоровтың теңдеулер жүйесін көрсетеді.

ҚОЖ үшін тәуекелдің пуассондық ағынында осы теңдеулер жүйесінің бастапқы шарттары $p_0(0) = 1, p_1(0) = 0$ мәндері болады.

Ал оның шешімдері келесі қатынастар болады:

$$p_0(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}; \quad (3.4)$$

$$p_1(t) = \frac{\mu}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}. \quad (3.5)$$

Осы қатынастардан ҚОЖ АҚБЖ-нің $t \to \infty$ шекті стационарлық режимі келесі ықтималдық мәндерімен сипатталатын болады:

$$p_0(t) = \frac{\mu_1}{\lambda_0+\mu_1}; \quad (3.6)$$

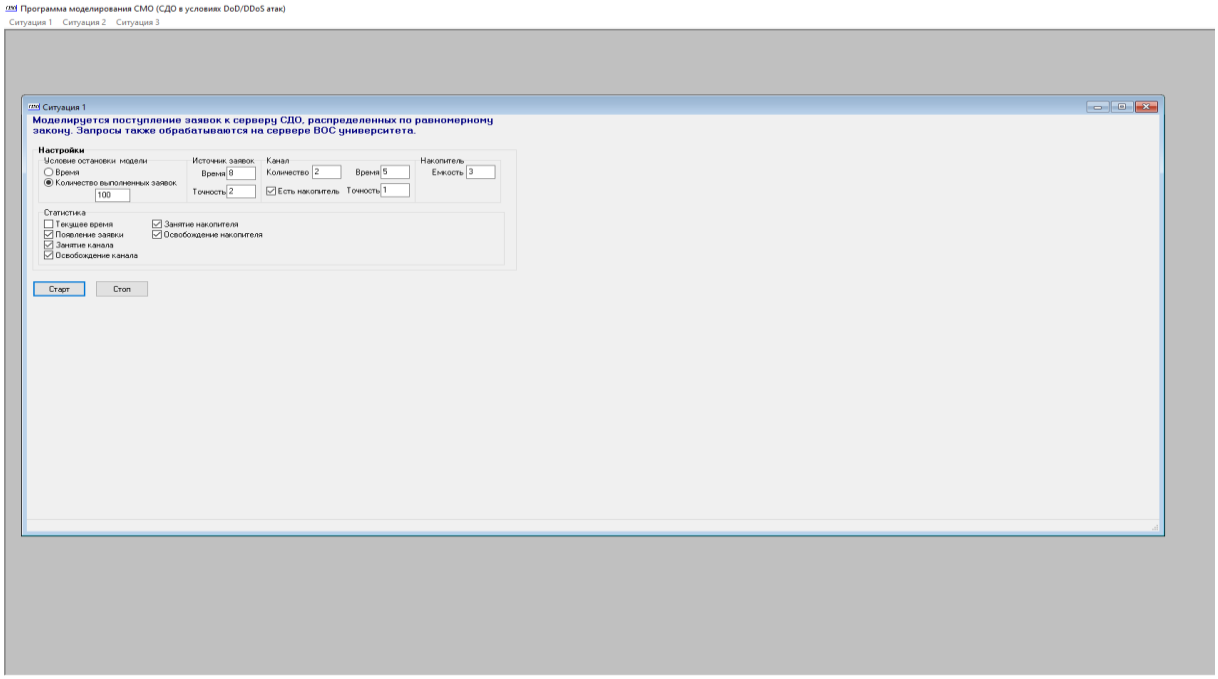
$$p_1(t) = \frac{\lambda_0}{\lambda_0+\mu_1}. \quad (3.7)$$

Осылайша, жоғарыда ҚОЖ-нің АҚБЖ-н ЖҚКЖ ретінде бейнелеудің ұқсастығы негізделген. Бұл олардың арасындағы құрылымдық және функционалдық ұқсастықтарды анықтаудың арқасында мүмкін болды. Олардың ішінде қызмет көрсетуге арналған сұраныстардың кіріс ағыны (тәуекелдерді өңдеу), кезектегі тәртіп және қызмет көрсету механизмдері ерекшеленеді. Осыған байланысты ҚОЖ-нің АҚБЖ бір фазалық бас тартумен ЖҚКЖ ретінде түсіндіруге болады.

Диссертацияның екінші тарауында сипатталған модельдерді жүзеге асыру үшін, сондай-ақ ЖҚКЖ-нің классикалық модельдері негізінде [100-102] ЖҚКЖ ретінде ҚОЖ-нің параметрлерін модельдеу үшін бағдарламалық өнім әзірленді, ол

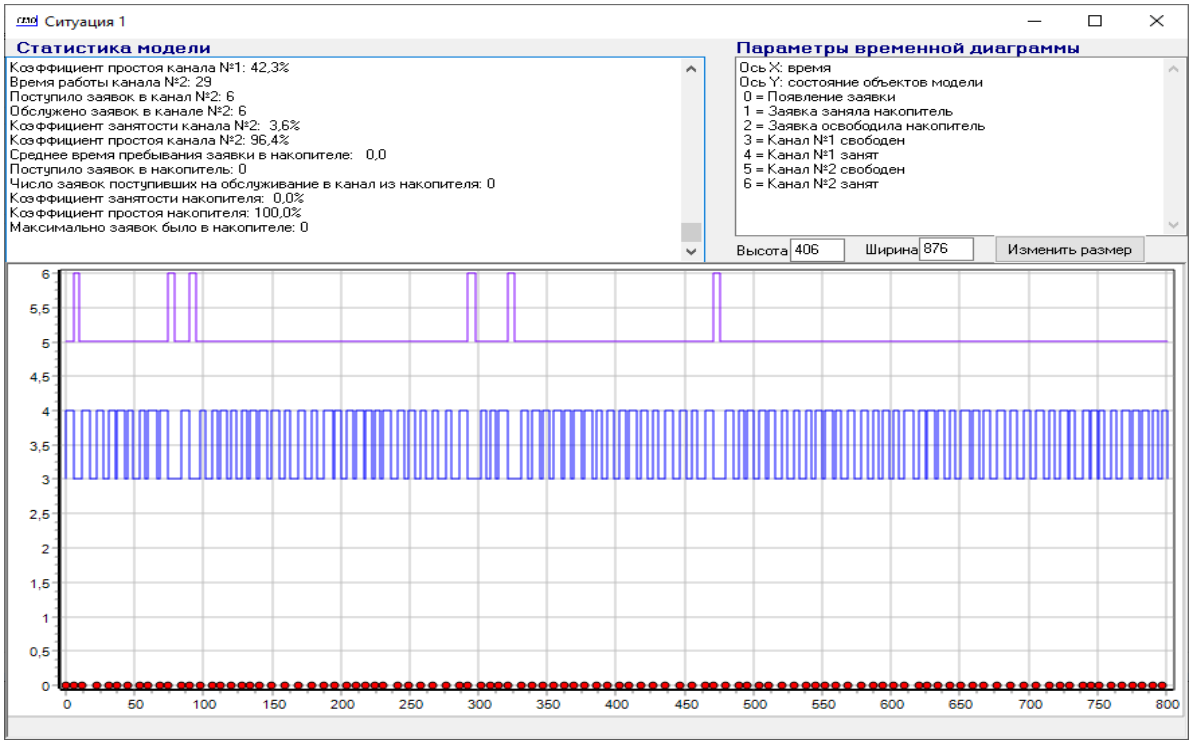
есептеу эксперименттері кезінде ҚОЖ және ВБО серверлеріне сұраныстарды визуализациялауға, сондай-ақ, сұраныстардың қарқындылық динамикасын модельдеуге мүмкіндік береді, мысалы, сыртқы және ішкі DoS/DDoS шабуылдар кезінде. Dos/DDoS шабуылдары ҚОЖ-не әсер етуді модельдеу нысаны ретінде - оларды оқу орындарына қарсы қолдану статистикасына сүйене отырып, сондай-ақ мұндай шабуылды жүзеге асыру шабуылдаушы тараптан жоғары біліктілікті талап етпейтіндігіне негізделіп таңдап алынды. Алайда мұндай шабуылдардың экономикалық зияны кез келген ұйым үшін айтарлықтай сезіледі.

23-27–суреттерде ЖҚКЖ ретінде ҚОЖ және оның АҚБЖ-нің жұмысын әр түрлі режимдермен модельдеу үшін «ModelSMO2020» (БӨ) бағдарламалық өнімінің негізгі интерфейстері көрсетілген.

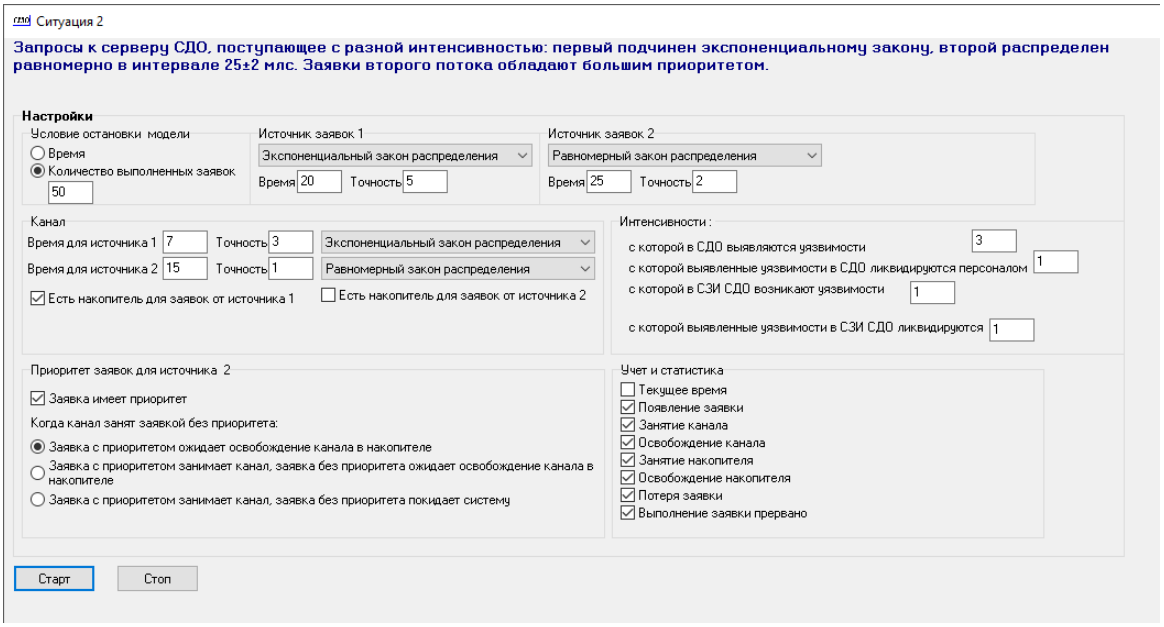


Сурет 23 – ЖҚКЖ ретінде ҚОЖ және оның АҚБЖ-нің жұмысын әр түрлі режимдерін модельдеуге арналған бағдарлама интерфейсінің жалпы түрі

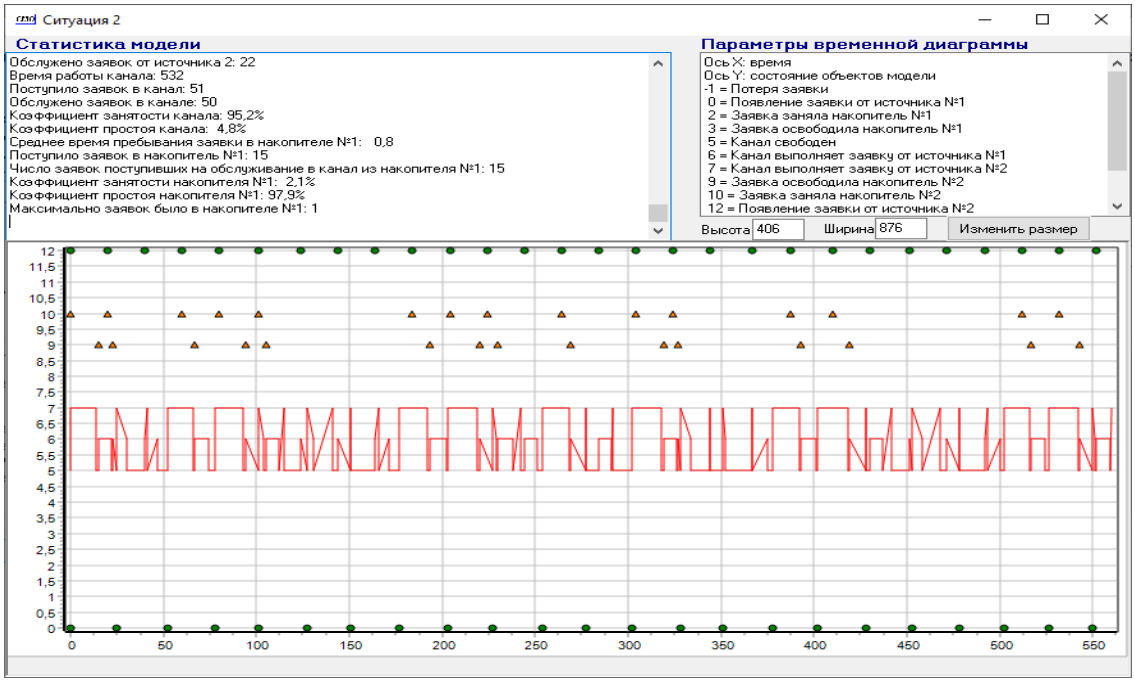
24, 26, 27 – суреттерінде сынық сызықтармен сұраныстардың түсімін бөлу тығыздық функциясының графиктері көрсетілген. Түрлі-түсті маркерлермен (үшбұрыштар мен нүктелер) қызмет көрсететін арналардағы сұраныстар мен дисперсияның мәндеріне сәйкес көрсетілген [99, p.1999-2000].



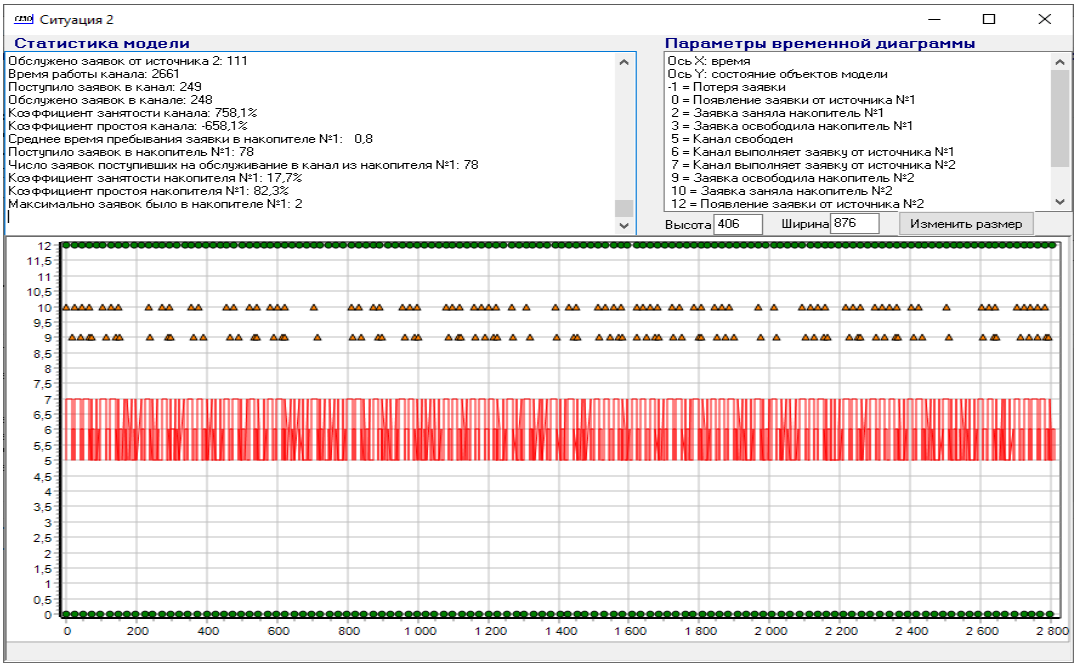
Сурет 24 – Бірқалыпты заң бойынша бөлінген ҚОЖ және оның АҚБЖ-не сұраныстардың түсуін модельдеу



Сурет 25 – ҚОЖ және оның АҚБЖ-не сұраныстардың түсуі экспоненциалды тарату заңы бойынша жүргізіледі және ағындардың біреуінің сұранысы неғұрлым жоғары басымдыққа ие жағдайының интерфейсі



Сурет 26 – ҚОЖ және оның АҚБЖ-не сұраныстардың келіп түсуін экспоненциалды тарату заңы бойынша және ағындардың біреуінің сұранысы неғұрлым жоғары басымдыққа ие жағдайын модельдеудің нәтижелері



Сурет 27 – ҚОЖ және оның АҚБЖ-не сұраныстардың келіп түсуін экспоненциалды тарату заңы бойынша және ағындардың біреуінің сұранысы неғұрлым жоғары басымдыққа ие жағдайын модельдеудің нәтижелері (Арна ҚОЖ-нің серверіне шабуыл жасау нәтижесінде 758% жүктеу коэффициентімен бос болмайды)

ЖҚКЖ ретінде ҚОЖ және оның АҚБЖ-нің жұмыс режимдерін модельдеу нәтижесінде көрсетілгендей, егер сұраныстардың кіріс ағынының таралу заңы біркелкі немесе қалыпты болса, онда жүйенің штаттық режімдерден ауытқуы байқалмайды. Алайда, егер ағындардың біріне неғұрлым жоғары басымдылық берсе (сурет 27), онда жағдай түбегейлі өзгереді. Атап айтқанда, ҚОЖ серверінің қалыпты конфигурациясы, мысалы, секундына 20-70 сұраныс түсуінің қарқындылығына арналған, олар сұраныстардың қалыпты қызмет көрсетуін қамтамасыз ете алмайды. Атап айтқанда, бір серверде секундына 100-120 сұраныс болғанда, жүктеу коэффициенті 700-800% жетеді.

Сондай-ақ, экспоненциалды заң шығыс деректерін барынша таратуға әкелетіні көрсетілген. Бұл тарату сұраныстардың кіріс ағындарының қарқындылық мәндеріне байланысты емес.

Осыған ұқсас есептеулер 4–кестеде көрсетілгендей тәуелділік негізінде ҚОЖ-нің АҚБЖ-н модельдеу жағдайы үшін де жүргізілді. Атап айтқанда, ҚОЖ АҚБЖ-нің жобалық сипаттамаларын модельдеу үшін ұсынылған бағдарламалық өнімнің кеңейтілген функционалдық мүмкіндіктері бар. Атап айтқанда, бағдарламалық өнім АҚБЖ сипаттамаларының мәнін есептеуді автоматтандыруды қамтамасыз ете алады және үлестірілген есептеу желісінің күрделі архитектурасы бар ірі ЖОО ҚОЖ-нің АҚБЖ-н жобалау кезінде тәуекелдерді басқару бойынша шешім қабылдау үшін пайдаланылуы мүмкін.

Кесте 4 – ЖОО ҚОЖ-нің АҚБЖ-не қойылатын жобалық талаптарды қалыптастыру

№	ЖОО-ның ҚОЖ-нің АҚБЖ-нің жобалық сипаттамалары	ҚОЖ-нің АҚБЖ-нің сипаттамаларын аналитикалық ұсыну
1	ҚОЖ-нің АҚБЖ-нің номиналды өнімділігі, $t_{\text{обработки}}$ өңдеу уақыты, μ_0 қызмет көрсету ағынының қарқындылығы.	$t_{\text{обработки}} = \frac{1}{\mu}$
2	ρ - ҚОЖ-нің АҚБЖ-і жүктемелерінің қарқындылығы	$\rho = \frac{\lambda}{\mu}$
3	ҚОЖ-нің АҚБЖ-і p_0 тәуекелін өңдей алмауы (ҚОЖ-нің АҚБЖ-нің тоқтап қалуының үлесі), Q салыстырмалы өткізу мүмкіндігінің ықтималдығы	$p_0 = \frac{\mu}{\lambda + \mu} = Q$
4	Қашықтықтан оқыту жүйесі үшін өңделген тәуекелге $p_{\text{отказа}}$ бас тарту ықтималдығы, $L_{\text{об}}$ уақыт бірлігінде өңделуі мүмкін тәуекелдердің орташа саны.	$p_{\text{отказа}} = \frac{\lambda}{\lambda + \mu} = L_{\text{об}}$
5	А Абсолюттік өткізу мүмкіндігі (қызмет көрсетілген сұраныстар ағынының қарқындылығы).	$A = \frac{\lambda\mu}{\lambda + \mu}$
6	АҚБЖ-нің тоқтап қалуының орташа уақыты $t_{\text{простоя}}$.	$t_{\text{простоя}} = \frac{\lambda}{\mu(\lambda + \mu)}$
7	ҚОЖ үшін киберқауіпсіздік және ақпараттық қауіпсіздік тәуекелдерінің саны, олар уақыт бірлігінде өңдеуден бас тартуы	$\frac{\lambda * \lambda}{\lambda + \mu}$

Эксперименттік зерттеу жүргізілді, ол қызмет көрсету ағынының берілген қарқындылығы кезінде $0{,}0001 < r_0 < 1$ диапазонда ҚОЖ-нің киберқауіпсіздік контурын еңсеру тәуекелі деңгейінің мәндері және бір шартты уақыт бірлігімен көрсетілген тәуекелді өңдеудің күтілетін уақыты үшін жүзеге асырылған. Нәтижелер ірі ЖОО-ның ҚОЖ-і үшін АҚБЖ-н жобалау процесінің тиімділігін қамтамасыз етуге мүмкіндік беретін жобалық сипаттамалар көрсеткіштерінің базасы түрінде қалыптастырылған.

$r_0 = 0{,}9;\ \mu = 1$ үшін АҚБЖ-нің параметрлерін есептеу мысалы 5–кестеде келтірілген. ЖҚКЖ ретінде ҚОЖ-нің АҚБЖ-н бейнелеудің дұрыстығы көрсетілген. Ол үшін тәуекелдердің кіріс ағыны λ қарқындылығымен пуассоновтық ретінде қарастырылған. Бұл тәуекелдер уақыттың кездейсоқ мезеттерінде пайда болатынын білдіреді, және де $(t, t + \Delta t)$ уақыт интервалында бір тәуекелдің пайда болу ықтималдығы t уақыт мезетіне тәуелді емес және $\lambda \cdot \Delta t$ тең екенін білдіреді.

Сонда ҚОЖ-не шабуылмен байланысты екі және одан да көп тәуекелдердің осы уақыт интервалында пайда болу ықтималдығы өте аз. Жекелеген кибер тәуекелдерді өңдеу ұзақтығы экспоненциалды тарату заңымен және $1/\mu$ өңдеудің орташа уақытымен кездейсоқ деп болжанады. Бұл $(t, t + \Delta t)$ уақыт интервалында кезекті кибер тәуекелдерді өңдеуді аяқтау ықтималдығы уақыт мезетіне тәуелді емес және $(\mu \cdot \Delta t)$ тең.

Кесте 5 – Киберқауіпсіздік контурларын еңсеру тәуекелінің белгілі бір қолайлы деңгейінде ҚОЖ-нің АҚБЖ-нің жобалық сипаттамалары $r_0 = 0{,}9;\ \mu = 1$

Өңдеу уақыты		1
ҚОЖ үшін кибер тәуекелдер ағынының қарқындылығы	λ	0,005176
АҚБЖ-дегі кибер тәуекелдерді өңдеу ағынының қарқындылығы	μ	1
АҚБЖ-нің жүктемелерінің қарқындылығы	ρ	0,0052
АҚБЖ-нің тоқтап қалу ықтималдығы	p_0	0,99485
АҚБЖ-нің тоқтап қалуының орташа уақыты		0,005149
Өңделмеген кибер тәуекелдердің үлесі	$p_{\text{необр.}}$	0,0052
АҚБЖ-нің абсолюттік өткізу қабілеті		0,00515
АҚБЖ-нің салыстырмалы өткізу қабілеті	Q	0,995
АҚБЖ- де өңделетін кибер тәуекелдердің орташа саны	$L_{\text{обр.}}$	0,0052

Осылайша, ЖҚКЖ ретінде ҚОЖ немесе ЖООЦББО-ры үшін АҚБЖ-нің ұсынылған моделінің интерпретация мүмкіндіктерін бұрыннан белгілі модельдермен салыстыру АҚБЖ-нің мұндай ұсынылуы басқа формальды

талаптарды (сандық жобалық сипаттамаларды) алу есебінен АҚБЖ-нің жобалық сипаттамаларында қолайлы кибернетикалық тәуекел деңгейінің интерпретациялау нәтижелерінің дұрыстығын арттыру арқылы жобалау процесінің үлкен тиімділігін қамтамасыз ететіндігін дәлелдейді.

Жүргізілген есептеу эксперименттері негізгі теориялық ережелердің, практикалық әзірлемелердің және жұмыстың осы тараудың қорытындыларының дұрыстығын растады.

А қосымшасында ЖҚКЖ ретінде ҚОЖ және оның АҚБЖ-н модельдеу үшін әзірленген бағдарламаның листингтері берілген.

Осылайша, диссертацияның осы тарауында ЖҚКЖ ретінде ҚОЖ-не және оның АҚБЖ-не талдау жүргізілді. Мұндай есептеу эксперименттері ҚОЖ-не сыртқы шабуылдардың әсерін неғұрлым дәл сипаттауға және ҚОЖ-рі үшін киберқауіпсіздік контурын құрудың ұтымды нұсқаларын таңдау мәселелерін талдап тексеруге мүмкіндік берді. Соңғысын, мысалы, диссертацияның екінші тарауында ұсынылған әдістер мен модельдерді қолдана отырып, ойындар теориясының қалыптасқан әдістерімен бірге жүзеге асыруға болады [106,107].

3.2 Антагонистік ойын негізінде қашықтықтан оқыту жүйесінің киберқауіпсіздік контурларын құру нұсқаларын оңтайландыру

Диссертацияның соңғы тарауында ЖОО-ның шектелген бюджеті жағдайында нөлдік сомамен дуэльдік ойын деп аталатын кибершабуылдан болатын потенциальды шығынды азайту критерийі бойынша ҚОЖ-н қорғаудың тиімді құралдарын таңдауға негіздеме жасалды. Сондай-ақ, осы тарауда жұмыстың екінші тарауында ұсынылған шабуыл қатерінің марковтық модельдеріне арналған имитациялық эксперименттердің нәтижелері келтірілген.

Міндеттің қойылуын айқындаймыз.

Қорғалуы әртүрлі бағдарламалық және аппараттық жабдықтарды (ақпаратты қорғау құралдары – АҚҚ) пайдалануды көздейтін ҚОЖ-нің желісі болсын, олардың тізімін және комбинациясын желінің администраторы оларды сатып алу мен пайдаланудың шектеулі бағаларын ескере отырып таңдайды.

ҚОЖ-нің желісі ақпараттың тұтастығын, құпиялылығын және қол жетімділігін бұзуға әкеп соғуы мүмкін осалдықтарға ие, соның нәтижесінде ЖОО-на материалдық шығын келтіріледі. Біз ҚОЖ үшін қатерлер белгілі априори (мысалы, CAPEC, ISACA, OWASP Top Ten және т.б. шабуылдар статистикасы мен кітапханаларының көмегімен) деп санаймыз.

Міндет келесіден тұрады: ҚОЖ үшін қатерлердің берілген векторында априори кезінде оқу орнының шектеулі бюджетімен кибер шабуылдың потенциальды шығынын азайту критерийі бойынша жергілікті және желілік қатерлерден ақпаратты қорғау құралдарының оңтайлы комбинациясын таңдау.

Киберқауіпсіздік қатерлерінің ағымдағы жағдайын және ақпаратты қорғау құралдарының көптүрлілігін, сондай-ақ ақпараттық ағындарды (1-тарау) ескере

отырып, сипатталған міндетті ойындар теориясының математикалық аппаратының көмегімен шешуге болады. Бұл ҚОЖ-н математикалық түрде қорғау бойынша міндетін қалыптастыруға мүмкіндік береді және қорғау тарапының оңтайлы стратегияларының критерийін пайдалана отырып, ЖОО-ның ақпараттық ресурстарының (АР) қауіпсіздігін қамтамасыз ету шығындарын есептеуге мүмкіндік береді. Сонымен қатар ҚОЖ-не шабуылдарды сәтті жүзеге асырудан болатын потенциальды шығындарды анықтауға және осы деректерді ескере оңтайлы шешім қабылдауға, атап айтқанда ақпаратты қорғау құралдарының тиімді жиынтығын таңдауға болады.

Қаскүнем мен администратордың (шешім қабылдайтын тұлға–ШҚТ) арасындағы қарым-қатынасты зерттеу олардың кейбір ойында ойыншылар болып табылатынын көздейді. Әрбір тарап өзінің қызығушылығын оңтайлы қамтамасыз етуге ұмтыла отырып, мінез-құлқының қандай да бір стратегиясын таңдай отырып, өз қадамдарын жасайды. Ойынның мақсаты администраторға қатысты да, қаскүнемге қатысты да мінез-құлықтың оңтайлы стратегиясын табу, себебі екі тарап, әдетте, өзінің сәтсіздіктерін азайтуға тырысады.

Бірінші кезеңде ҚОЖ-нің АР-н қорғаудың неғұрлым тиімді стратегияларын іздеу үшін екі тараптың математикалық дуэльдік бинарлық ойынын өткізу қажет. 1-тарап–ақпаратты қорғау жүйесі. 2–тарап–қаскүнемдердің ықтимал шабуылдары. Негізгі мақсат – қауіпсіздік администраторымен оңтайлы қорғаныс стратегиясын анықтау, ал шабуылдаушылардың мақсаттары маңызды емес, сондықтан қаскүнем ҚОЖ-не мүмкіндігінше көп зиян келтіруге тырысады деп есептеуге болады.

Қауіпсіздік администраторының стратегиясы ретінде біз ойын матрицасының $S_i(i=1,...,n)$ қатарын, ал қаскүнемдің стратегиясы ретінде – оның $A_j(j=1,...,m).$ бағандарын түсінеміз.

ҚОЖ-нің АҚБЖ администраторының стратегияларына ақпаратты қорғаудың түрлі құралдарын және олардың бір-бірімен мүмкін болатын барлық комбинацияларын жатқызуға болады. Қаскүнемнің стратегиялары - ҚОЖ-не жергілікті және желілік шабуылдардың түрлері. Матрицаның элементтері ақпаратты қорғау құралдарының мүмкін болатын комбинацияларының бірі қолданылған жағдайда p_{ij} қаскүнемнің шабуылының сәтті жүзеге асырылу ықтималдығы. Айта кету керек, ықтималдықтар тек жаңа ғана емес, сонымен қатар ҚОЖ-де бар ақпаратты қорғау құралдарымен (мұндай бар болған жағдайда) пайдаланылатынын ескере отырып қойылады. Бұл соңына келгенде қарсы шараларды (ҚОЖ-н қорғау стратегиясы: екінші тарауда сипатталған $\lambda_i, \mu_i,$ ескере отырып, қаржылық, техникалық, ұйымдастырушылық) таңдауға мүмкіндік береді.

Ақпаратты қорғау құралдары комбинациясының элементтері бір-бірінен тәуелсіз деп болжанады. Атап айтқанда, олардың біреуінің жұмысы немесе дұрыс жұмыс істемеуі екіншісіне әсер етпейді. Мысалы, өшірілген антивирус файрволдың жұмысына әсер етпейді. Сондықтан, [108] теоремасына сүйене

отырып, бірнеше тәуелсіз оқиғалардың үйлесу ықтималдығы осы оқиғалардың ықтималдығының көбейтіндісіне тең болады. ҚОЖ үшін ақпаратты қорғаудың түрлі құралдарының комбинацияларын пайдалану кезінде шабуылдарды табысты жүзеге асыру ықтималдығы келесідей болады: $P(AB) = P(A) \cdot P(B)$.

Мұндай болжамда екі тараптың ойыны үшін матрицаны аламыз, оның нұсқасы 6–кестеде келтірілген, мұнда S_0 қатары – ҚОЖ-де ақпаратты қорғаудың ағымдағы құралдарын (пайдаланылған априори) қолдану кезінде шабуылдарды табысты жүзеге асыру мүмкіндігі.

Кесте 6 – Ойынның бастапқы матрицасы

	A_1	A_2	...	A_m
S_0	p_{01}	p_{02}	...	p_{0m}
S_1	p_{11}	p_{12}	...	p_{1m}
S_2	p_{21}	p_{22}	...	p_{2m}
...	...	...	...	...
S_n	p_{n1}	p_{n2}	...	p_{nm}
S_{1+2}	$p_{11} \cdot p_{21}$	$p_{12} \cdot p_{22}$	...	$p_{1n} \cdot p_{2m}$
...	...	...	...	...

Сонымен қатар, $p_j^{(A)}$ шабуылының әрбір типін орындау ықтималдығы белгілі, мысалы, ақпаратты ауыстыру немесе ҚОЖ- нің виртуалдық желісіне DDoS шабуылы. Бұл ықтималдықтардың мәні статистикалық деректерге байланысты. Сондай-ақ $X_i (i = 1,...,n)$ ақпаратты қорғау құралдарының әрқайсысының құны және $Y_j (j = 1,...,m)$ белгілі бір шабуылды жүзеге асырудан болған болжамды шығынның мөлшері бағаланды.

Қатерлер мен осалдықтарды жүзеге асыру ықтималдығын бағалау процесіне ерекше назар аудару қажет (2-тарауды қараңыз). Бұл кезеңді орындауды ішкі қызметкерлер тобына да, сыртқы сарапшыларға да тапсыруға болады.

Әртүрлі компьютерлік жүйелерді, мысалы, шешім қабылдауды қолдау жүйелерін немесе сараптамалық жүйелерді қолдануға болады. Сондай-ақ, ұйымның өзінің сараптамалық деректерін ғана емес, мысалы, ҚОЖ-нің администраторын немесе ЖОО-ның ақпараттық білім беру орталарын пайдалану қажет, сонымен қатар ақпараттық және киберқауіпсіздік бойынша талдау агенттіктері жүргізетін қатерлер статистикасын ескеру қажет [109].

Ақпаратты қорғаудың белгілі бір құралдарын енгізудің мақсатқа сәйкестігі туралы шешім қабылдау үшін, шабуылды табысты жүзеге асыру кезіндегі потенциальды шығындарды, ақпаратты қорғау құралдарын енгізу кезіндегі потенциальды пайданы, сондай-ақ ҚОЖ-нің киберқауіпсіздігінің барлық

контурларын енгізуге және жұмыс істеу қабілетін қолдауға арналған нақты шығындарды ескеру қажет.

Сонымен, келесі қадам инвестицияны бағалау көмегімен, атап айтқанда, 5 – кестенің әрбір элементі үшін инвестицияны қайтару көрсеткіші (*ROI*) арқылы осы есепті шешу, ол былайша есептеледі:

$$ROI_{ij} = \text{benefits}_{ij} - \text{costs}_{\text{ij}}, \quad (3.8)$$

мұнда benefits_{ij} – j-ші шабуылын жүзеге асыру кезінде ақпаратты қорғаудың і-ші құралын енгізуде әкелетін пайданы(атап айтқанда , потенциальды шығындардың төмендеуін күту) бағалау;

costs_{ij} – ҚОЖ-де ақпаратты қорғаудың і-ші құралын жұмысқа қабілеттілігін енгізу және қолдау шығындары.

ҚОЖ үшін потенциальды шығындардың төмендеуін күтуді бағалау келесі формула бойынша есептеледі:

$$\text{benefits}_{ij} = R_{0j} - R_{\text{ij}}, \quad (3.9)$$

мұнда R_{0j} – ағымдағы ақпаратты қорғаудың құралдарын (ҚОЖ-де пайдаланылатын априори) пайдалану кезіндегі j-ші кибершабуылдарды жүзеге асыру кезіндегі потенциальды шығындар;

R_{ij} – і - ші ақпараттық қорғау құралын пайдаланып, j-ші кибершабуылдарды жүзеге асыру кезіндегі потенциальды шығындар.

ҚОЖ-рі үшін потенциальды шығындар қаскүнемнің шабуылды табысты жүзеге асыруының p_{ij} ықтималдығын ескере отырып есептеледі (шабуыл жүз пайыздық ықтималдықпен жүргізілетін жағдайда). Есептеу кезінде, сондай-ақ, шабуылдың белгілі бір типін жүзеге асырудың $p_j^{(A)}$ ықтималдығы, сондай-ақ белгілі бір шабуылды жүзеге асырудан келтірілген Y_j. шығын мөлшері ескеріледі, содан кейін біз келесі өрнекті аламыз:

$$R_{\text{ij}} = p_{ij} \cdot p_j^{(A)} \cdot Y_j. \quad (3.10)$$

ҚОЖ үшін i – ші ақпаратты қорғаудың құралдарымен жұмысқа қабілеттілікті енгізу және қолдау шығындары X_i.-ге тең.

Демек, ROI_{ij} есептеу формуласының соңғы нұсқасы келесідей:

$$ROI_{ij} = p_{0j} \cdot p_j^{(A)} \cdot Y_j - p_{ij} \cdot p_j^{(A)} \cdot Y_j - X_i = \left(p_{0j} - p_{ij}\right) \cdot p_j^{(A)} \cdot Y_j - X_i. \quad (3.11)$$

Бастапқы матрицаның әрбір элементі үшін *ROI* -ді есептеп, ойынның жаңа матрицасын аламыз (кесте 7), мұнда матрица элементтері шабуылдың белгілі бір түріне қатысты ҚОЖ-де нақты ақпаратты қорғаудың құралдарын енгізудің артықшылықтарының сандық сипаттамасы.

Кесте 7 – Бастапқы матрицаның әрбір элементі үшін ROI-ді қайта есептегеннен кейінгі ойын матрицасы

	A_1	A_2	...	A_m
S_0	ROI_{01}	ROI_{02}	...	ROI_{0m}
S_1	ROI_{11}	ROI_{12}	...	ROI_{1m}
S_2	ROI_{21}	ROI_{22}	...	ROI_{2m}
...	...	...	...	...
S_n	ROI_{n1}	ROI_{n2}	...	ROI_{nm}

Келесі қадам-алынған матрицаның шешімі болады. Зерттеулер көрсеткендей, мұндай матрицаларды жуықтап шешу үшін Браун-Робинсон итеративтік әдісін қолдануға болады [108, с.328].

Жоғарыда айтылғандарды ескере отырып, қолданыстағы матрица үшін осы ойынды қайталаудың шексіз процесін қарастырамыз, онда әрбір қадамда ойыншылардың әрқайсысы қарсылас алдыңғы қадамдарда таза стратегиялардың пайда болу жиілігімен анықталатын аралас стратегияны таңдайды, ал өзі осы болжам бойынша ең жақсы нәтижені қамтамасыз ететін таза стратегияны таңдайды.

Бірінші ойыншы (немесе ҚОЖ-н қорғаушы) $i_1,...,i_k$ таза стратегиясын, ал екінші ойыншы (қаскүнем) $j_1,...,j_k$ таңдаған ойынның k рет қайталануы орындалды делік. Содан кейін, жоғарыда айтылғандарға сәйкес, бірінші ойыншы келесі шарттан $(k+1)-$ші қадамында i_{k+1} стратегиясын таңдайды:

$$\frac{1}{k}\sum_{\nu=1}^{k} a_{i_{k+1} j_\nu} = \max_{1\le i\le n} \frac{1}{k}\sum_{\nu=1}^{k} a_{ij_\nu} = \nu_1(k), \qquad (3.12)$$

мұнда $k-$ қадам номері; $a_{ij}-$ ойын матрицасының элементі; $n-$ бірінші ойыншының стратегияларының саны; $\nu-$ ойын бағасы.

Ал екінші ойыншы j_{k+1} стратегиясын келесідей шарттан таңдайды:

$$\frac{1}{k}\sum_{\nu=1}^{k} a_{i_\nu\, j_{k+1}} = \max_{1\le j\le m} \frac{1}{k}\sum_{\nu=1}^{k} a_{i_\nu j} = \nu_2(k), \qquad (3.13)$$

мұнда $k-$қадам номері; $a_{ij}-$ ойын матрицасының элементі; $m-$ екінші ойыншының стратегияларының саны; $\nu-$ ойын бағасы.

Егер сәйкес шарттарға жауап беретін бірнеше стратегиялар болса, онда ойыншы олардың кез келгенін таңдайды.

Осылайша, итеративті процесс ойынның шынайы мәніне ауысады, атап айтқанда:

$$\lim_{k\to\infty} v_1(k) = \lim_{k\to\infty} v_2(k) = v. \qquad (3.14)$$

Алынған өрнек $v_1(k)$ және $v_2(k)$- v ойынның нақты бағасына ұмтылатындығын білдіреді, бұл біздің жағдайда ҚОЖ үшін ақпаратты қорғау құралдарын құрудың оңтайлы стратегиясы.

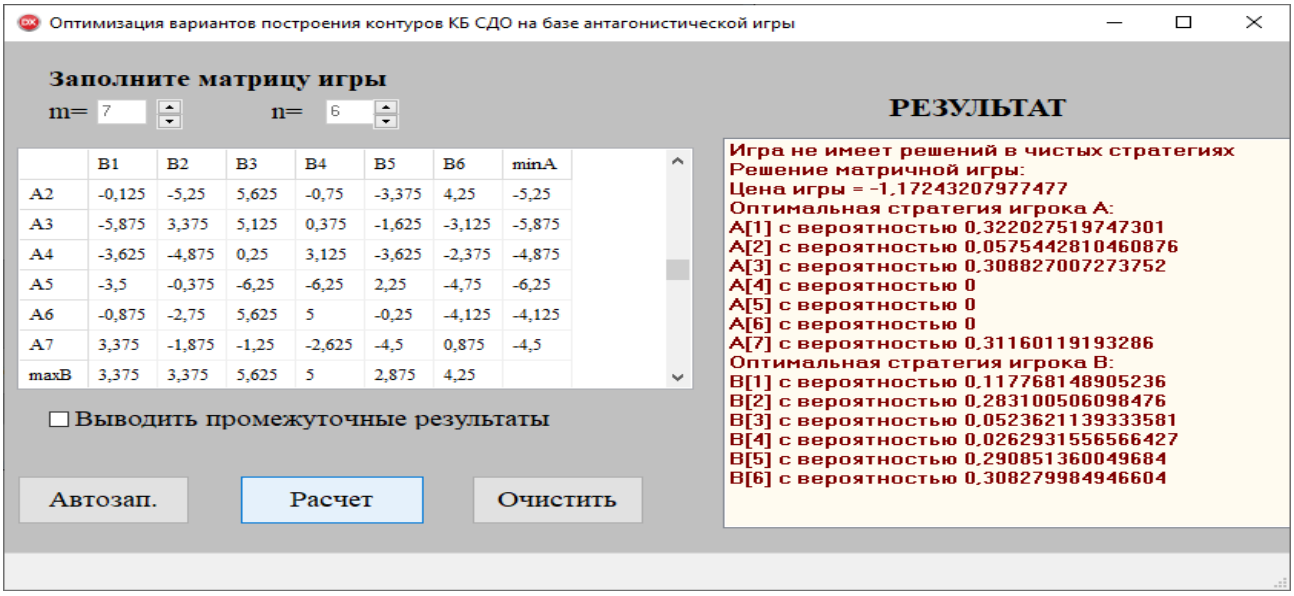
Айта кету керек, [108, с.330] сәйкес, бұл итеративті әдістің жинақталуы баяу, бірақ әдістің өзі өте қарапайым және белгілі бір дәрежеде ҚОЖ үшін ақпаратты қорғау құралдарын құру нұсқаларын моделдеу кезінде қақтығыс жағдайының көптеген қайталануы нәтижесінде тәжірибені қорғау тарапын иемдену процесін көрсетеді.

Антагонистік ойын матрицасын есептеу үшін бастапқы деректердің мысалы, жалпы ЖОО немесе ҚОЖ, факультеттердің ақпараттық желілері үшін тиімді ақпаратты қорғаудың құралдарын іздеу процесі 8–кестеде көрсетілген. Жүйе ҚОЖ және ВБО үшін екі сервері бар, аудиторияның он коммутаторы қосылған бір негізгі коммутатор. Сонымен қатар, жүйеде аудиториялар желісін басқаруға, ВБО-на мамандандырылған бағдарламаларды орналастыруға және т.б. арналған серверлер бар. Аудиториядағы ДК-лер мен жұқа клиенттер саны 60-тан 100-ге дейін өзгеруі мүмкін.

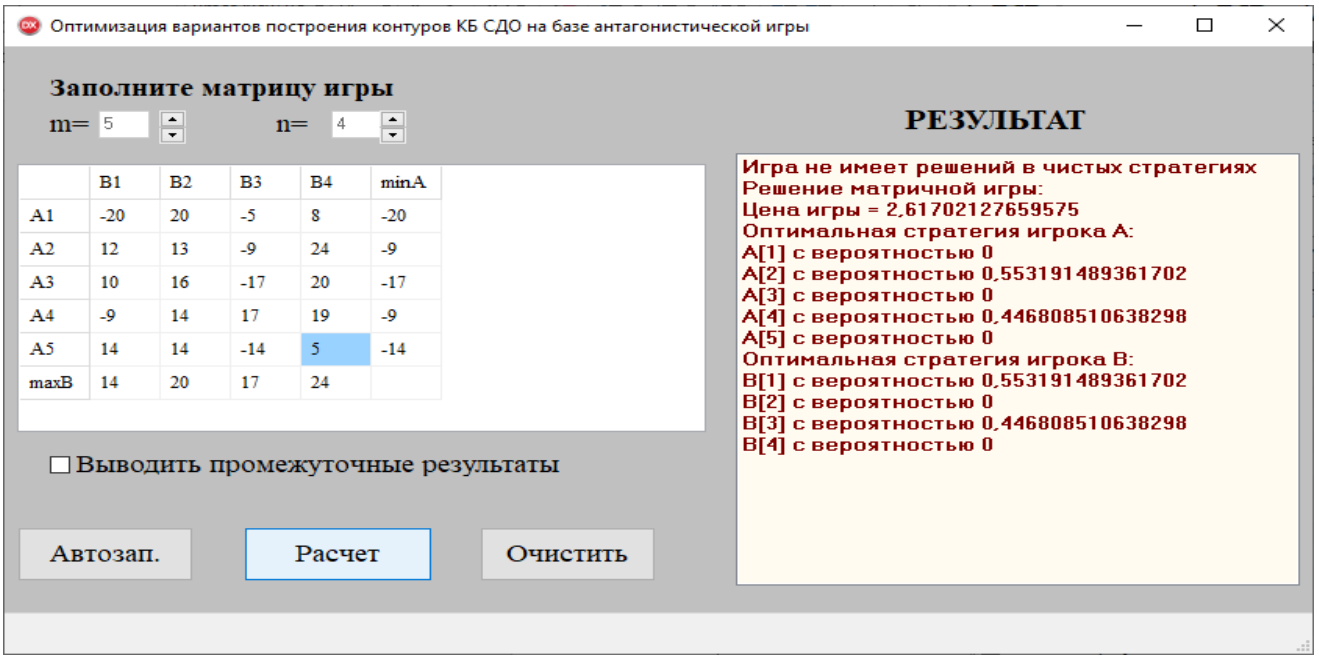
Кесте 8 – Факультеттің желілік төбелерінің сипаттамасы

№	Төбе түрі	Саны	Киберқауіпсіздік үшін қатерлер			
			вирустық	сыртқы шабуыл	ішкі шабуыл	электрқуатын беруде жаңылу мүмкіндігі
			Төбедегі ақпаратты қорғау құралдарына арналған инвестицияларды қайтару көрсеткіші (у.е.)			
			Өндіруші мен рейтингке байланысты: антивирус, резервтік көшіру үшін брандмауэр бағдарламалық қамтамасыз ету және т.б.			
1	Факультеттің сервері	2	2-10	0.6-2.5	0.6-3.5	1.5-2.5
2	Негізгі коммутаторлар	1	0.2-1	0.2-1	0.2-1	0.2-0.5
3	Аудиторияның коммутаторлары	10	0.2-1	0.2-1	0.2-1	0.2-1
4	ВБО, ҚОЖ және т.б. серверлері	2-5	0.5-100	0.2-100	0.1-100	0.4-100
5	Жергілікті компьютерлер және жұқа клиенттер	60-100	0.5-10	0.4-10	0.7-20	0.4-10

Зерттеу барысында «Matrix_2020» бағдарламасы әзірленді (28 және 29-суреттер), ол ақпаратты қорғаудың әртүрлі құралдарына инвестицияларды қайтарудың берілген деңгейлері кезінде қорғау тарапының ең жақсы стратегиясын іздеуді автоматтандыруға мүмкіндік береді.



Сурет 28 – «Matrix_2020» бағдарламасы интерфейсінің жалпы түрі



Сурет 29 – «Matrix_2020» бағдарламасы интерфейсінің жалпы түрі

«Matrix_2020» бағдарламасы RAD Studio 10.3 бағдарламалау ортасында жүзеге асырылған, интуитивті түсінікті интерфейске ие және ҚОЖ-нің киберқауіпсіздік контурында ақпаратты қорғау құралдарының әртүрлі үйлесімдерін алдын ала талдау үшін қолдануға болады. Ә қосымшасында бағдарламаның листингі көрсетілген.

Ойын матрицасы ақпаратты қорғаудың белгілі бір құралдарын енгізгеннен түскен кірісті есептегеннен кейін немесе ақпаратты қорғау құралдарын

пайдаланбаған кезде шығынға әкелетін жағдайда толтырылады (бұл жағдайда сәйкес ұяшыққа «-» белгісі қойылады).

Ұяшықтардағы мәндер нақты ақша валютасына байланыстырмай, шартты бірліктерде көрсетілген.

Мысалы, 29 – суретте ҚОЖ үшін антивирустық бағдарламалық қамтамасыз етуді таңдау нұсқасы үшін антагонистік ойын матрицасы көрсетілген (кесте 9).

Кесте 9 – ҚОЖ үшін антивирустық бағдарламалық қамтамасыз етуді таңдау нұсқасы үшін антагонистік ойын матрицасы фрагментінің мысалы

АҚБЖ администраторының стратегиялары (таңдалған антивирустық бағдарламасы)	Тәуелсіз тесттер нәтижесінде БҚЕ рейтингі	Құны, шарт. бірл.	Кешенділік
Avira Pro	95	75	Ия
Антивирус Касперского	98	100	Ия
Comodo Security	92	0	Ия
Bitdefender Free	98	0	Жоқ
Panda Security	85	60	Ия

ЖҚКЖ-нің модельдеріне және антагонистік ойын негізінде ҚОЖ-нің киберқауіпсіздік контурын құру нұсқаларын оңтайландыру модельдеріне ұсынылған толықтыруларды ескере отырып, шектеулі бюджет жағдайында ҚОЖ-нің киберқауіпсіздік контурын және АҚБЖ-н қалыптастыру әдістемесі толықтырылды. ЖҚКЖ ретінде ҚОЖ-нің киберқауіпсіздігін басқаруды қалыптастыру әдістемесі келесі кезеңдерді қамтиды:

1. ҚОЖ-нің нақты архитектурасын анықтау. Бұл кезеңде ҚОЖ-нің (немесе ЖООЦББО) төбелерінің саны және олардың өзара әрекеттесу механизмдері, мысалы, ақпараттық ағындары бар ақпараттық желілер (1-тарауды қараңыз) және ВБО (1-тарауды қараңыз) анықталады;

2. ҚОЖ-не арналған ақпаратты қорғау құралдарының контурына жалпы қойылатын шектеулерді анықтау (мысалы, ақпаратты қорғау құралдарының максималды құнын жалпы шектеу, жергілікті шектеу, мысалы, ҚОЖ-нің серверлерін немесе АҚБЖ-не жүгінулер саны бойынша ВБО-ның серверлерін жүктеу және т. б.);

3.Жалпы ҚОЖ-нің киберқатерлері мен осалдықтарының тізімін қалыптастыру. Киберқатерлердің әртүрлі кластарын қолдану нәтижесінде болуы мүмкін потенциальды шығынды есептеу;

4. ҚОЖ-нің ақпараттық қауіпсіздігі мен киберқауіпсіздігі үшін басымдылық тәуекелдердің сипаттамасы. ЖҚКЖ ретінде ҚОЖ-нің АҚБЖ-нің сипаттамасы.

Жаппай қызмет көрсету жүйесімен құрылымдық, мазмұнды және функционалды ұқсастығы бар ҚОЖ-нің АҚБЖ-нің параметрлерін анықтауға арналған модель есебінен ЖОО-ның ҚОЖ-і үшін АҚБЖ-нің көптеген сандық сипаттамалары қалыптастырылады. Осылайша, осы кезеңде ҚОЖ-і үшін АҚБЖ-н жобалау процесінің тиімділігі қамтамасыз етіледі;

5. ҚОЖ үшін ақпаратты қорғау құралдарының кластарын анықтау. Мысалы, ақпаратты қорғау құралдарының кластарына аутентификация және идентификация құралдары, антивирустық БҚЕ және т. б. жатады;

6. Ақпараттық желілер мен ҚОЖ-не шабуылдар қатерін және ақпараттық желілер мен ҚОЖ-де киберқатерді анықтаудың жетілдірілген әдісін сипаттайтын көрсеткіштерді есептеу моделі негізінде (2-тарауды қараңыз), кластағы таңдалған ақпаратты қорғау құралдары киберқатердің ықтималдығын және жүзеге асырылған кибершабуылдың потенциальды шығынының мөлшерін төмендететінін анықтаймыз;

7. Антагонистік ойын моделінің көмегімен ҚОЖ үшін ақпаратты қорғау құралдарының тиімділігін анықтаймыз;

8. Біз алдыңғы кезеңдерге сүйене отырып, ҚОЖ-не ақпаратты қорғау құралдарын қолданудың ең оңтайлы нұсқасын есептейміз;

9. ЖҚКЖ ретінде ҚОЖ-н моделдеудің негізінде бір фазалық бас тартумен ЖҚКЖ ретінде АҚБЖ қалыптастырылады.

Үшінші тарау бойынша қорытындылар

Диссертациялық жұмыстың үшінші тарауында келесідей нәтижелер алынды:

– жаппай қызмет көрсету жүйесі (ЖҚКЖ) ретінде қашықтықтан оқыту жүйесінің ақпараттық қауіпсіздікті басқару жүйесімен сипаттаудың ұқсастығы анықталды. Бұл қашықтықтан оқыту жүйесі мен жаппай қызмет көрсету жүйесінің арасындағы құрылымдық және функционалдық ұқсастықтарын анықтаудың арқасында мүмкін болды. Мұндай түсіндірудің салдары ЖҚКЖ ретінде ҚОЖ-нің АҚБЖ-нің бастапқы талаптарды модельдеу және қалыптастыру мүмкін екендігі көрсетілді. АҚБЖ бір фазалық бас тартумен ЖҚКЖ ретінде түсіндіруге болатындығы көрсетілді;

– жаппай қызмет көрсету жүйесінің параметрлерін анықтау үшін модельдер одан әрі дамытылды, ол құрылымдық, мазмұндық, функционалдық ұқсастықтар есебінен ЖОО-ның қашықтықтан оқыту жүйелері үшін ақпараттық қауіпсіздікті басқару жүйесінің көптеген сандық сипаттамаларын қалыптастыруға мүмкіндік береді және де ол компьютерлік қаскүнемдер тарапынан қашықтықтан оқыту жүйесіне деструктивті әсерлердің саны мен күрделілігінің өсу перспективаларын ескере отырып, жоғары оқу орындары үшін ақпараттық қауіпсіздікті басқару жүйесін жобалау процесінің тиімділігін қамтамасыз етуге мүмкіндік береді;

– ЖҚКЖ ретінде ҚОЖ-і үшін АҚБЖ-нің сипаттамалары түсіндірілді. АҚБЖ-нің мұндай формалданған моделі басқа формальды талаптарды (сандық жобалық

сипаттамаларды) алу есебінен АҚБЖ-нің жобалық сипаттамаларында қолайлы кибернетикалық тәуекел деңгейінің интерпретациялау нәтижелерінің дұрыстығын арттыру арқылы жобалау процесінің үлкен тиімділігін қамтамасыз ететіндігі көрсетілген;

– негізгі теориялық ережелер мен практикалық зерттемелердің дұрыстығын растайтын есептеу эксперименттері жүргізілді;

– ҚОЖ-нің киберқауіпсіздік және ақпаратты қорғау жүйесін құрудың оңтайлы жолын таңдау әдістемесі одан әрі дамыды, әдістеменің басқаларынан айырмашылығы, ақпараттық желіде және ҚОЖ-де киберқатерді анықтаудың жетілдірілген әдісімен, ЖҚКЖ ретінде ҚОЖ-нің ақпараттық қауіпсіздігін басқару жүйесінің моделімен, оқу орнының шектеулі бюджеті жағдайында ақпаратты қорғау құралдарын тиімді және ұтымды іздеу үшін антагонистік ойын моделімен толықтырылған.

ҚОРЫТЫНДЫ

Жүргізілген диссертациялық зерттеулер негізінде келесі нәтижелер алынды:

– қазіргі ЖОО–ның цифрлық білім беру ортасын және оның компоненттері - қашықтықтан оқыту жүйесін (ҚОЖ) киберқорғау тәсілдері талданды. ҚОЖ-нің виртуалдық бұлттық ресурстар мәселерінің функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету міндеттері зерттелді. Ақпаратты қорғау жүйесіне және ақпараттандырудың әртүрлі нысандарының киберқауіпсіздігіне, соның ішінде ҚОЖ-не және жалпы ЖООЦББО-на инвестициялаудың тиімділігін бағалау үшін қолданыстағы модельдерге талдау жасалды. Осы саладағы зерттеулердің көпшілігі ақпаратты қорғау жүйесінде қаржы ресурстарын салудың оңтайлы стратегияларын іздеу мәселесін экономикалық тұрғыдан қоюға ғана назар аударылғаны көрсетілген және ҚОЖ-нің және ЖООЦББО-ның киберқауіпсіздігінде инвестициялық жобалар үшін шешімдер қабылдау және бақылау процедурасына ақпараттық технологияларды енгізуге қатысты тенденцияларды ескермейді;

– жоғары оқу орындарының қашықтықтан оқыту жүйелеріндегі ақпараттық ағындарды ұйымдастыру құрылымы ұсынылған, ол қашықтықтан оқыту жүйесінде айналымдағы ақпараттық ағындарды бақылау мен өңдеудің қазіргі және жаңа перспективалы механизмін кешенді өзара әрекеттесу тиімділігін арттыруға қабілетті;

– ҚОЖ-не шабуылдардың қаупін сипаттайтын, көрсеткіштер үшін ақпаратты қорғау жүйелерін сипаттау бойынша мәселелерді шешу моделі алынды. Ол ҚОЖ-не және ЖООЦББО-на шабуыл қатерлерінің нақты дұрыс марковтық модельдерін құруға болады. ҚОЖ-нің киберқауіпсіздігін инвестициялаудың ұтымды стратегиясын таңдау модельдері мен алгоритмдерімен бірге ҚОЖ-н қорғалған және функционалды тұрақтылығын құру әдіснамасын жетілдіруге болатындығы көрсетілген;

– ҚОЖ-де киберқатерді анықтау әдісі жетілдірілді. Жетілдірілген әдіс, қолданыстағыларына қарағанда, киберқатерлер түріне байланысты бөлінген желілік өзін-өзі оқыту және қарсы шараларды таңдау рекурсивті алгоритмдерін (атап айтқанда, қашықтықтан оқыту жүйесінің ақпараттық желісін қорғау тараптары үшін қаржылық немесе техникалық стратегияларды) қамтиды. Киберқатерлерді анықтау әдістеріне ұсынылған толықтыруларды іске асыру қашықтықтан оқыту жүйесінің қорғалу дәрежесін жақсарту үшін қажетті қарсы шаралар туралы негізделген шешімдерді шығаруды жүзеге асыруға мүмкіндік береді. Бұл ретте қашықтықтан оқытудың жүйесінде әр түрлі көздерден келіп түсетін нақты уақытта қашықтықтан оқыту жүйесін басқару мақсаттарының динамикалық өзгеруі жағдайында киберқауіпсіздік туралы ақпарат талданады;

–Ақпараттандыру нысандарының бағдарламалық-конфигурацияланатын желілері үшін ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздігін

қамтамасыз ету үшін математикалық модельдері жетілдірілді. Модель кибершабуыл параметрлерінің виртуалдық ВБР-на әсерін ескере отырып жетілдірілді. Сондай-ақ модельде ВБР-дың күйін және бағдарламалық-конфигурацияланатын желілер үшін кешенді көрсеткіш негізінде мүмкін болатын қарсы шаралар таңдау ескеріледі. Виртуалдық бұлттық ортаға шабуыл графы әзірленді, ол жүйенің барлық белгілі осалдықтары туралы ақпарат алуға мүмкіндік береді, сонымен қатар ВБР-ның функционалды тұрақтылығы мен киберқауіпсіздігінің күйін нақты уақыт режимінде көрсетеді. Ұсынылған модельдерді кешенді қолдану нәтижесінде ақпараттандыру нысандарының ақпараттық қауіпсіздік администраторына ықтимал киберқатер мен шабуылдарды, атап айтқанда, виртуалдық бұлттық желісінде анықталған оқиғаларды корреляциялау есебінен болжауға болады. Бұлттық ортадағы қатерлерді талдау үшін алгоритмдер әзірленді, бұл жұмыстың нәтижесінде виртуалдық бұлттық ортасына шабуыл жасаудың бір немесе бірнеше жолын алу; қарсы шара таңдау, оның нәтижесі ақпараттандыру нысанына және оның ВБР-на шауылдың нақты сценарийі үшін қарсы шараны таңдау;

– бағдарламалық-конфигурацияланатын желілерді қолдану негізінде ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету әдістемесі ұсынылды. Бұл әдістеме виртуалдық желілерді қайта конфигурациялау және кибершабуылдарды анықтау негізінде виртуалдық машиналардың компрометациясының тұрақтылығын арттыруға бағытталған. Әзірленген әдістеме мен модельдерге эксперименталды апробация жүргізілді. Алынған нәтижелердің адекватылығын растау үшін тестілік виртуалдық бұлттық орта іске асырылды. Ұсынылған шешімдер жалпы алғанда ҚОЖ-н және ВБО-ның функционалды тұрақтылығы мен киберқауіпсіздік көрсеткішін белгілі шешімдермен салыстырғанда 12-17%-ға арттыруға мүмкіндік беретіні эксперименталды көрсетілді;

– ҚОЖ-нің ақпараттық қауіпсіздікті басқару жүйесін жаппай қызмет көрсету жүйесі (ЖҚКЖ) ретінде бейнелеудің ұқсастығы анықталған. Мұндай түсіндірудің салдары ЖҚКЖ ретінде ҚОЖ-нің АҚБЖ-нің бастапқы талаптарды модельдеу және қалыптастыру мүмкіндігі болуы мүмкін екендігі көрсетілген. АҚБЖ бір фазалық бас тартумен ЖҚКЖ ретінде түсіндіруге болатындығы көрсетілгін. Жаппай қызмет көрсету жүйесінің параметрлерін анықтау үшін модельдер одан әрі дамытылды, ол құрылымдық, мазмұндық, функционалдық ұқсастықтар есебінен ЖОО-ның қашықтықтан оқыту жүйелері үшін ақпараттық қауіпсіздікті басқару жүйесінің көптеген сандық сипаттамаларын қалыптастыруға мүмкіндік береді және де ол компьютерлік қаскүнемдер тарапынан қашықтықтан оқыту жүйесіне деструктивті әсерлердің саны мен күрделілігінің өсу перспективаларын ескере отырып, жоғары оқу орындары үшін ақпараттық қауіпсіздікті басқару жүйесін жобалау процесінің тиімділігін қамтамасыз етуге мүмкіндік береді. ЖҚКЖ ретінде ҚОЖ-і үшін АҚБЖ-нің сипаттамаларын түсіндірілген. АҚБЖ-нің

мұндай формалданған моделі басқа формальды талаптарды (сандық жобалық сипаттамаларды) алу есебінен АҚБЖ-нің жобалық сипаттамаларында қолайлы кибернетикалық тәуекел деңгейінің интерпретациялау нәтижелерінің дұрыстығын арттыру арқылы жобалау процесінің үлкен тиімділігін қамтамасыз ететіндігі көрсетілген. Негізгі теориялық ережелер мен практикалық зерттемелердің дұрыстығын растайтын есептеу эксперименттері жүргізілді;

– ҚОЖ-нің киберқауіпсіздік және ақпаратты қорғау жүйесін құрудың оңтайлы жолын таңдау әдістемесі одан әрі дамыды, әдістеменің басқаларынан айырмашылығы, ақпараттық желіде және ҚОЖ-де киберқатерді анықтаудың жетілдірілген әдісімен, ЖҚКЖ ретінде ҚОЖ-нің ақпараттық қауіпсіздігін басқару жүйесінің моделімен, оқу орнының шектеулі бюджеті жағдайында ақпаратты қорғау құралдарын тиімді және ұтымды іздеу үшін антагонистік ойын моделімен толықтырылған.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Akhmetov B., Lakhno V., Malyukov V., Sarsimbayeva S., Kartbayev T., Doszhanova A., Abuova A. Automation of decision making support on the distribution of financial resources on the elimination of accidents // International Journal of Civil Engineering and Technology. –2019, – Vol. 10, No.3, –P.2716-2724.

2 Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Математические основы компьютерной безопасности // ПДМ. - 2019, № 44, -С.43–57.

3 Марков А.С., Барабанов А.В., Цирлов В.Л. О систематике информационной безопасности цепей поставки программного обеспечения // Безопасность информационных технологий. –2019. –Т. 26. № 3. –С. 68-79.

4 Зегжда П.Д. Систематизация киберфизических систем и оценка их безопасности // Зегжда П.Д., Полтавцева М.А., Лаврова Д.С. Проблемы информационной безопасности. Компьютерные системы. – 2017. № 2. –С. 127-138.

5 Korchenko A. Akhmetov B., Kazmirchuk S., Chasnovskiy Ye. Система оценивания рисков информационной безопасности // Information security risk assessment system – «RISK-CALCULATOR» // Ukrainian Scientific Journal of Information Security. –2017. –Vol. 23. Iss. 2. – P. 145-152.

6 Tukeyev U., Toporov V., Axelrod V. Online Monitoring System of the Enrichment Factory Input Ore Flows Quality on the Base of Temporal Model // Springer International Publishing AG. Springer Nature. – 2018. -P. 1–11.

7 Atighetchi M, Simidchieva B., Carvalho M., Last D. Experimentation Support for Cyber Security Evaluations // CISRC '16: Proceedings of the 11th Annual Cyber and Information Security Research Conference. –2016. –N.5. –P. 1–7.

8 Campbell R.H., Yan M., Sprabery R., Gopireddy B., Fletcher C.W. Attack directories, not caches: Side channel attacks in a non-inclusive world // IEEE Symposium on Security and Privacy. Institute of Electrical and Electronics Engineers Inc. –2019. –P. 888-904.

9 Dawkins J., Clark K., Manes G., Papa M. A Framework for Unified Network Security Management: Identifying and Tracking Security Threats on Converged Networks // Journal of Network and Systems Management. –2005. –Vol.13. N.3. –P. 253–267.

10 Балықбаев Т.О., Бидайбеков Е.Ы., Ахметов Б.С., Гриншкун В.В. Абай атындағы Қазақ ұлттық педагогикалық университетін цифрландыру тұжырымдамасы. –2020. –97б.

11 Ахметов Б.С., Лахно В.А., Адранова А.Б. Университеттердің қашықтықтан білім беру жүйесін қорғаудың өзекті мәселелері мен міндеттері // Респ ғыл.-прак. конф. материалдары «Өндірістегі цифрлық технологиялар». – Актау. – 2019. –Б.300-303.

12 Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны»). Қазақстан Республикасы Үкіметінің 2017 жылғы «30» маусым № 407 қаулысымен бекітілген. –2017. –29 б.

13 Лебедева М.Б. Массовые открытые онлайн-курсы как тенденция развития образования //Человек и образование. –2015. –№1(42).

14 Akhmetov B., Lakhno V., Adranova A.B., Kydyralina L.M. Review and analysis of previous researches in the sphere of ensuring the protection of information and educational environment of universities // Bulletin of National Academy of Sciences of the Republic of Kazakhstan. –2019. –V.4. N. 380. –P.154 – 169.

15 Ахметов Б.С., Лахно В.А., Адранова А.Б., Кыдыралина Л.М. Жоғары оқу орнының ақпараттық білім беру ортасын қорғау құралдарын таңдаудың векторлық оңтайландыру модельдері мен алгоритмдері // Хабаршы Абай атындағы ҚазҰПУ, «Физика-математика ғылымдары»сериясы. – 2018. – Алматы. –№1(61). –Б.243-248.

16 Ахметов Б.С., Алимсеитова Ж.К., Адранова А.Б. Стратегия развития дистанционного образования КазНПУ имени Абая в рамках проекта «Цифровой университет»// Вестник КазНПУ, Серия «Физико-математические науки». – 2018. – Алматы. –№2(62). –С.46-49.

17 Ахметов Б.С., Алимсеитова Ж.К., Адранова А.Б.. Организация дистанционного обучения в КазНПУ имени Абая // Вестник КазНПУ, Серия «Физико-математические науки». – 2018. – Алматы. –№4(64). –С.124-127.

18 Котенко Д.И., Котенко И.В., Саенко И.Б. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Тр. СПИИРАН. –2012. –Т. 3(22). – С.5–30.

19 Koller D., Friedman N. Probabilistic Graphical Models // Principles and Techniques. MIT Press. – 2009.

20 Котенко И.В., Степашкин М.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Тр. ИСА РАН. – 2007. – Т.31. – С.126–207.

21 Росенко А.П. Внутренние угрозы безопасности конфиденциальной информации: Методология и теоретическое исследование. М: Изд-во Красанд. – 2010.

22 Иванов К.В., Тутубалин П.И. Марковские модели защиты автоматизированных систем специального назначения //Республиканский центр мониторинга качества образования. – М.:Казан. – 2012.

23 Карпов В.В. Вероятностная модель оценки защищенности средств вычислительной техники с аппаратно-программным комплексом защиты информации от несанкционированного доступа// Программные продукты и системы. – 2003. – № 1. – С.31–36.

24 Щеглов К.А., Щеглов А.Ю. Марковские модели угрозы безопасности информационной системы // Изв. вузов. Приборостроение. –2015. –Т.58. № 12. – С. 957–965.

25 Щеглов К.А., Щеглов А.Ю. Математические модели эксплуатационной информационной безопасности // Вопросы защиты информации. –2014. – Т.106. № 3. – С.52–65.

26 Щеглов К.А., Щеглов А.Ю. Интерпретация и моделирование угрозы атаки на информационную систему. Часть 1. Моделирование угрозы уязвимости и интерпретация угрозы атаки // Информационные технологии. –2015. – Т.21. № 12. – С.930–940.

27 Щеглов К.А., Щеглов А.Ю. Интерпретация и моделирование угрозы атаки на информационную систему. Часть 2. Моделирование угрозы атаки // Информационные технологии. – 2016. – Т. 22. № 1. –С.54–64.

28 Адранова А.Б. Защита информационных ресурсов систем дистанционного обучения в университетах // Труды сатпаевских чтений «Инновационные технологии – ключ к успешному решению фундаментальных и прикладных задач в рудном и нефтегазовом секторах экономики РК». – 2019. – Алматы. –С.395-397.

29 Вергазов Р.И. Система автоматизированного дистанционного тестирования / Вергазов Р.И., Гудков П.А. // Новые информационные технологии: Тез. докл. Восьмая межд. студенческая школа семинар. 2000. –Крым.

30 Ложников П.С. Распознавание пользователей в системах дистанционного образования / П. С. Ложников // Educational Technology & Society. –2001. – № 4.

31 Махутов Б.Н. Защита электронных учебников в дистанционном обучении / Махутов Б.Н., Шевелев М.Ю.// Образование XXI века: инновационные технологии, диагностика и управление в условиях информатизации и гуманизации: Мат. III Всероссийской науч.-метод. Конф. с межд. участием. –2001. – Красноярск. – С.106 – 108.

32 Мочалов А.А. Эффективный менеджмент системы дистанционного образования / Мочалов А.А., Степанов П.А. // Сб. науч. работ. –2010. – №5(434). – С.130–133.

33 Jakobson G. Mission-centricity in cyber security: Architecting cyber attack resilient missions // 5th International Conference on Cyber Conflict. –2013. P. 1–18.

34 Al Dairi A. Cyber security attacks on smart cities and associated mobile technologies // Procedia Computer Science. –2017. –Vol.109. –P.1086–1091.

35 Sherzer E., Gilboa-Freedman G., Levy H. Resource allocation in a cloud under virus attacks // In VALUETOOLS. –2017. –P.223–224.

36 Nguyen M., Samanta P., Debroy S. Analyzing Moving Target Defense for Resilient Campus Private Cloud //11th International Conference on Cloud Computing. – 2018. –P.114–121.

37 Qi J., Hahn A., Lu X., Wang J., Liu C.C. Cybersecurity for distributed energy resources and smart inverters // IET Cyber-Physical Systems: Theory & Applications. – Vol.1(1). –28–39.

38 Brown C.J., Dog S.E., Edwards S.P., Mc Nab N.C., Steele M., Franklin J.M. Mobile Device Security: Cloud and Hybrid Builds // (No. Special Publication (NIST SP)-1800-4). –2019.

39 Adelmeyer M., Teuteberg F. Cloud Computing Adoption in Critical Infrastructures-Status Quo and Elements of a Research Agenda // Proceedings. –2018. – P.1345–1356.

40 Amann P., Klayn A., Mounier G. Changing the rules of the game: How can law enforcement deter criminals by increasing the risks of conducting cybercrime? // Cyber Security: A Peer-Reviewed Journal. –2017. –Vol.1(1). –P.16–27.

41 Адранова А.Б. Концепция организации информационных потоков систем дистанционного образования с учетом необходимости обеспечения их 4кибербезопасности // Вестник КазНИТУ. –2019. –№6(136). –С. 460-465.

42 Адранова А.Б. Цифрлық білім беру ортасының виртуалды бұлтты ресурстарының функционалды тұрақтылығы мен киберқауіпсіздігін қамтамасыз ету // IX Халық. ғыл.-әдіст. конф. «Математикалық модельдеу мен ақпараттық технологиялар білімде және ғылымда». –2020. –Алматы. –Б.162-166.

43 Tamimi A.A., Dawood R., Sadaqa L. Disaster Recovery Techniques in Cloud Computing //Jordan International Joint Conference on Electrical Engineering and Information Technology. –2019. –P.845-850.

44 Duncan B., Happe A., Bratterud A., Sen J. Cloud Cyber Security: Finding an Effective Approach with Unikernels // Security in Computing and Communications; IntechOpen: London. –2017. –UK. P.31.

45 Akinsanya O.O., Papadaki M., Sun L. Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud? // In CERC. –2019. P.211–222.

46 Jouini M., Rabai L.B.A. A security framework for secure cloud computing environments // In Cloud security: Concepts, methodologies, tools, and applications. – 2019. –P. 249–263.

47 Khan N., Al-Yasiri A. Cloud security threats and techniques to strengthen cloud computing adoption framework // In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications. –2018. P. 268–285.

48 Bharadwaj D. R., Bhattacharya A., Chakkaravarthy M. Cloud Threat Defense–A Threat Protection and Security Compliance Solution// IEEE International Conference on Cloud Computing in Emerging Markets. –2018. P. 95–99.

49 Yeboah-Boateng E.O. Cyber-Security Concerns With Cloud Computing: Business Value Creation and Performance Perspectives // In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications. –2018. P. 995–1026.

50 Srinivasan S., Raja K. An Advanced Dynamic Authentic Security Method for Cloud Computing // In Cyber Security. –2018. –Singapore. P.143–152.

51 Masip-Bruin X., Marin-Tordera E., Jukan A., Ren G.J. Managing resources continuity from the edge to the cloud: Architecture and performance // Future Generation Computer Systems. –2018. –Vol.79. –P.777-785.

52 Wang L., Liu A., Jajodia S. Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts // Computer communications. –2016. –Vol.29(15). –P.2917–2933.

53 Amato F., Moscato F., Moscato V., Colace F. Improving security in cloud by formal modeling of IaaS resources// Future Generation Computer Systems. –2018. –Vol.87. –P.754–764.

54 Ахметов Б.Б., Адранова А.Б., Кыдыралина Л.М., Касымбергибаев Б. Проблематика развития теоретико-методических основ проектирования кибербезопасной облачно ориентированной учебной среды университета// I Міжнародна науково-практична конференція «Безпека ресурсів інформаційних систем». –2020. –Чернгів. –С.44-46.

55 LakhnoV. Development of the decision making support system to control a procedure of financial investment//V.A. Lakhno, V.Malyukov, N. Gerasymchuk // Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 6. №3. –P. 24-41.

56 Lakhno V.A. Development of a support system for managing the cybersecurity // Radio Electronics, Computer Science, Control. – 2017. – Vol.2. –P.109–116.

57 Gordon L. The Economics of Information Security Investment / L. Gordon, M. Loeb // ACM Transactions on Information and System Security. – 2002. – Vol.5. №4. – P.438-457.

58 Akhmetov B.B., Lakhno V.A., Adranova A.B., Kydyralina L.M., Pliska L.D. Analysis of mathematical models of investment strategies in the university on cyber security systems // Bulletin of national academy of sciences of the republic of Kazakhstan. – 2020. –№1(383). –P.128 – 139.

59 Hausken K. Returns to nformation Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability // Information Systems Frontiers. –2006. –N.5(8). –P.338-349.

60 Willemson J. On the Gordon & Loeb Model for Information Security Investment // Proceedings of The Fifth Workshop on the Economics of Information Security. –2006. –P.101-112.

61 Willemson J. Extending the Gordon & Loeb Model for Information Security Investment // Fifth International Conference on Availability, Reliability, and Security. –2010. –P.258-261.

62 Gordon L.A., Loeb M.P. Lucyshyn W. Zhou L. Externalities and the Magnitude of Cyber Security Under investment by Private Sector Firms: A Modification of the Gordon-Loeb Model // Journal of Information Security. –2015. –Vol.6. –P.24-30.

63 Shim W. Vulnerability and Information Security Investment under Interdependent Risks: a Theoretical Approach // Asia Pacific Journal of nformation Systems. - 2011. -Vol.21. - N. 4.

64 Shim W. Interdependent risk and cybersecurity: Ananalysis of security in vestmentand cyberinsurance // Michigan State University, EastLansing. –2010.

65 Zadiraka V.K. New Models and Methods for Estimating the Cryptographic Strength of Information Security Systems //Cybernetics and Systems Analysis. – 2017. – Vol.53. N.6. –P. 978-985.

66 Hlushak V.V. Syntez struktury systemy zahystu informacii z vykorystannjam pozycijnoi gry zahysnyka ta zlovmysnyka// Systemni doslidzhennja ta informacijni tehnologii. –2013. – №2. – P. 89-100.

67 Hlushak V.V., Novikov O.M. Metod proektuvannja systemy zahystu informacii z vykorystannjam determinovanoi gry “zahysnyk-zlovmysnyk” // Naukovi visti NTUU "KPI". –2011. –№ 2. –P. 46-53.

68 Levchenko Ye.G. Model Grossa v protystojannidvohstorin u sferizahystu informacii // Suchasna specialnatehnika. –2009. – №3(18). – P.75-81.

69 Gryschuk R.V. Hierarchical differential-gaming model for evaluation efficiency of information systems protection // Informatics & Mathematical Methods in Simulation. –2011. – №2.

70 Arkhypov O. Methods and Approaches to Investigating Information Risks by Means of Economic Cost Models // The Advanced Science Journal. –2014. –№2(12). – P.75-82.

71 Arhypov O.Y. Informacijni ryzyky: metody ta sposoby doslidzhennja, modeli ryzykiv I metody ih identyfikacii // Zahyst informacii. – 2013. – №4. –P.366-375.

72 Prus R.B. Formation of the objective function in the tasks of information security management // The Fourth World Congress ―Aviation in the XXI-st Century‖ Safety in Aviation and Space Technologies. –2010. –P.14 –17.

73 Levchenko Ye.G. Matematychni modeli ekonomichnogo menedzhmentu informacijnoi bezpeky / Ye.G. Levchenko, M.V. Demchyshyn, A.O. Rabchun // Systemni doslidzhennja ta informacijni tehnologii. –2011. – №4. –P.88-96.

74 Levchenko Ye.G. The correlation of expenses in multi-barrier information security systems / Ye. G. Levchenko, D.I. Rabchun// System research and information technologies. –2015. –№ 2. –P.131–140.

75 Levchenko Ye.G. Optymizacijni zadachi menedzhmentu informacijnoi bezpeky / Ye.G. Levchenko, A.O. Rabchun // Suchasnyj zahyst informacii. –2010. –№1. –P.16-23.

76 Akhmetov B.B., Lakhno V.A., Malyukov V.P. Model of investment strategies in cyber security systems of transport situational centers // Scientific journal Radio Electronics, Computer Science, Control. –2018. –Vol.2(45). –P. 83.

77 Алиев Т.И. Основы моделирования дискретных систем // СПб: Изд-во СПбГУ ИТМО. –2009.

78 Вентцель Е.С. Исследование операций //М: Сов. Радио. –1972.

79 Al-Jarrah O., Arafat A. Network Intrusion Detection System using attack behavior classification //5th International Conference on Information and Communication Systems. –2014.

80 Beketova G., Akhmetov B., Korchenko A. Simulation modeling of cyber security systems in Matlab and Simulink // Bulletin of the national academy of sciences of the republic of Kazakhstan. –2017. –Vol.3. –P.54–64.

81 Ben–Asher Gonzalez N.C. Effects of cyber security knowledge on attack detection // Computers in Human Behavior. –2015. –Vol. 48. –P. 51–61.

82 Nishanov, A. Kh, Kerimov, K.F. Methods of Counteraction from Attacks Carried out Against Users in a Network the Internet // ICEIC-Electronics, news and communications, IX-the conference. –2008. –Tashkent. –P.298–299.

83 Gamal M.M., Hasan B., Hegazy A.F. A Security Analysis Framework Powered by an Expert System // International Journal of Computer Science and Security. –2011. –Vol. 4. N.6. –P.505–527.

84 Chang Li-Yun, Lee Zne-Jung. Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system // International Conference on Fuzzy Theory and Its Applications. –2013. –P.346 – 351.

85 Kanatov M., Atymtayeva L., Yagaliyeva B. Expert systems for information security management and audit // Implementation phase issues, Soft Computing and Intelligent Systems, Joint 7th International Conference on and Advanced Intelligent Systems. –2014. –P. 896 – 900.

86 Lee Kuo-Chan, Hsieh C.H., Wei L.J., Mao C.H., Dai J.H., Kuang Y.T. Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation // Soft Computin. –2016. –P.1–14.

87 Lakhno V., Kazmirchuk S., Kovalenko Y., Myrutenko L., Zhmurko T. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features //Eastern-European Journal of Enterprise Technologies. –2016. –Vol.3/9(81). –P.30–38.

88 Louvieris P., Clewley N., Liu X. Effects-based feature identification for network intrusion detection // Neurocomputing. –2013, –Vol.121. Iss.9. –P.265–273.

89 Wang Z., Zhou X., Yu Z., He Y., Zhang D. Inferring User Search Intention Based on Situation Analysis of the Physical World // Chapter Ubiquitous Intelligence and Computing. –2010. –Vol.6406. –P. 35–51.

90 Akhmetov B. Designing a decision support system for the weakly formalized problems in the provision of cybersecurity // Eastern-European Journal of Enterprise Technologies. –2017. –Vol.1. –Iss.2(85). –P.4–15.

91 Adranova A., Lakhno V., Akhmetov B., Kystaubayeva A., Mussagulova G. Modeling of cyber threats in information networks of distance education systems // Journal of Theoretical and Applied Information Technology.– 2019. –Vol.97. –Iss. 18. –P.4921-4933.

92 Lakhno V.A. Algorithms for Forming a Knowledge Base for Decision Support Systems in Cybersecurity Tasks // Advances in Intelligent Systems and Computing // – 2020. –Vol.938. –P. 268–278.

93 Akhmetov B., Balgabayeva L. Mobile platform for decision support system during mutual continuous investment in technology for smart city // Studies in Systems, Decision and Control. –2019. –Vol.199. –P.731–742.

94 Akhmetov B., Lakhno V., Akhmetov B., Myakuhin Y., Adranova A., Kydyralina L. Models and Algorithms of Vector Optimization in Selecting Security Measures for Higher Education Institution's Information Learning Environment //Intelligent Systems in Cybernetics and Automation Control Theory. Advances in Intelligent Systems and Computing. –2019. –Vol.860. –P.135-142.

95 Akhmetov B.S., Lakhno V.A., Malyukov V.P., Doszhanova A.A., Alimseitova Zh.K. Adaptive Model of Cybersecurity Financing with Fuzzy Sets of Threats and Resources at the Protection Side // International Journal of Advanced Trends in Computer Science and Engineering. –2020. –Vol.9, N.4. –P. 5046 – 5052.

96 Gordon L.A., Loeb M.P., Zhou L. Investing in cybersecurity: Insights from the Gordon-Loeb model // Journal of Information Security. –2016. –Vol.7. –P.49.

97 Gordon L.A., Loeb M.P., Lucyshyn W., Zhou L. The impact of information sharing on cybersecurity underinvestment: A real options perspective // Journal of Accounting and Public Policy. –2015. –Vol.34 (5). –P. 509–519.

98 Akhmetov B., Lakhno V., Tkach Y., Adranova A., Zhilkishbayeva G. Problems of Development of a Cloud-Oriented Educational Environment of the University // International Journal of Advanced Trends in Computer Science and Engineering. – 2020. Vol.9. –Iss. 2. –P. 2196-2203.

99 Adranova A., Yona L., Kryvoruchko O., Desiatko A., Palahuta K., Blozva A., Gusev B. Methodology forming for the approaches to the cyber security of information systems management // Journal of Theoretical and Applied Information Technology.– 2020. –Vol.98. –Iss. 12. –P.1993-2005.

100 Susanto H., Almunawar M.N., Tuan Y.C. Information security management system standards: A comparative study of the big five // International Journal of Electrical Computer Sciences. –2011. –Vol.11(5). –P.23-29.

101 Ахметов Б.С., Лахно В.А., Малюков В.П., Адранова А.Б. Теория игр в задачах управления финансированием в кибербезопасность // Респ. науч.-прак. конф. «Современные информационно-коммуникационные технологии в образовании науке и практике» в рамках третьей модернизации Казахстана. – 2018. –Алматы. –С.406-407.

102 Шабанов А.П. Ось адаптивного управления: «информационная система– организационные структуры массового обслуживания» // Бизнес-информатика. – 2010. –Т.3.

103 Головко Н. И. Исследование моделей систем массового обслуживания в информационных сетях // Сибирский журнал индустриальной математики. –2008. –Т.11(2). –С. 50-64.

104 Павелкина К.И., Федотова Р.И. Современные тенденции развития DDoS-атак и защита от них // Информационные системы и технологии: управление и безопасность. –2014. – Т.3. –С. 226-232.

105 Файзуллин Р.Р., Байрушин Ф.Т. Защита от DOS-и DDOS-атак // Аллея науки. –2018. –Т.1(2). –С.786-788.

106 Абденов А.Ж. Заркумова Р.Н. Выбор средства эффективной защиты с помощью методов теории игр // Вопросы защиты информации. –2010. –Т.2. –С. 26-31.

107 Шматова Е.С. Выбор стратегии ложной информационный системы на основе модели теории игр // Вопросы кибербезопасности. – 2015. Т.5 (13).

108 Корн Г.А. Справочник по математике для научных работников и инженеров. – М: Наука. –1974. –С.832.

109 Пижевский Д. Е. Анализ мировой тенденции роста киберугроз на основе линейной аппроксимации статистических данных об атаках // Студенческая наука для развития информационного общества. –2019. –Р. 118-127.

ҚОСЫМША А

Адранова Асельхан Багдатовнаның диссертациялық
жұмысының нәтижелерін ендіру туралы
АКТ

Комиссия құрамы:

Комиссия төрағасы - Сахиев С.Қ., Абай атындағы Қазақ ұлттық педагогикалық университетінің Ғылыми жұмыс және цифрландыру жөніндегі проректорының м.а.

Комиссия мүшелері:

Серікбаев Т.К. – Абай атындағы Қазақ ұлттық педагогикалық университеті, Білімді ақпараттандыру департамент директорының орынбасары.

Бидайбеков Д.Е. – Абай атындағы Қазақ ұлттық педагогикалық университеті, біліктілікті арттыру және қашықтықтан білім беру орталығы директорының орынбасары.

Шапиев Ж.Е. – Абай атындағы Қазақ ұлттық педагогикалық университеті, бағдарламамен қамтамасыз ету бөлімінің бастығы.

Адранова Асельхан Багдатовнаның 6D060200 – «Информатика» мамандығы бойынша философия ғылымдарының докторы (PhD) дәрежесін алу үшін дайындаған «Қашықтықтан оқытудың ақпараттық қауіпсіздігін қамтамасыз етудің модельдері, әдістері және алгоритмдері» тақырыбындағы диссертация аясында жасалған бағдарламаларды ендіру үшін осы акт жасалып, төмендегі нәтижелер ендірілді, атап айтқанда:

1. Жаппай қызмет көрсету жүйесі ретінде қашықтықтан оқыту жүйесі және оның ақпараттық қауіпсіздікті басқару жүйесінің жұмысын әр түрлі режимдермен модельдеу үшін «ModelSMO2020» бағдарламасы, ол қашықтықтан оқыту жүйесі және виртуалдық бұлттық орта серверлеріне сұраныстарды визуализациялауға, сондай-ақ, сұраныстардың қарқындылық динамикасын модельдеуге мүмкіндік береді;

2. Оқу орнының шектеулі бюджеті жағдайында ақпаратты қорғау құралдарын тиімді және ұтымды іздеу үшін антагонистік ойын моделімен «Matrix_2020» бағдарламасы, ол ақпаратты қорғаудың әртүрлі құралдарына инвестицияларды қайтарудың берілген деңгейлері кезінде қорғау тарапының ең жақсы стратегиясын іздеуді автоматтандыруға мүмкіндік береді.

Төраға:

ҒЖжЦ жөніндегі проректорының м.а. С.Қ. Сахиев

Комиссия мүшелері :

БАД директорының орынбасары Т.К. Серікбаев

БАжҚББО директорының орынбасары Д.Е. Бидайбеков

БҚЕ бөлімінің бастығы Ж.Е. Шапиев

ҚОСЫМША Ә

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

03041, м. Київ, вул. Героїв Оборони, 16, навчальний корпус № 15, тел./факс: (044) 527-83-52,
E-mail: o-glazunova@nubip.edu.ua

017 № 16-34
На № _____ **від** 12.05.2020 р.

Акт
о внедрении результатов диссертационной работы
Адрановой Асельхан Багдатовны

Комиссия в составе:

председатель – декан факультета информационных технологий Национального университета биоресурсов и природопользования Украины (НУБИП), д.пед.н. проф. Глазунова Е.Г.

члены комиссии: д.т.н., проф. Лахно В.А., д.ф.-м.н., проф. Малюкова В.П.

составила настоящий акт, о том, что результаты теоретических и экспериментальных исследований, проведенных в рамках диссертационной работы Адрановой Асельхан Багдатовны «Модели, методы и алгоритмы обеспечения информационной безопасности дистанционного обучения», позволили апробировать и внедрить в учебном процессе факультета ИТ НУБИП Украины следующие результаты:

1) Модели и алгоритмы обеспечения кибербезопасности виртуальных облачных ресурсов для программно-конфигурируемых сетей системы дистанционного обучения вуза;
2) Компьютерная модель системы управления информационной безопасностью дистанционного образования университета как системы массового обслуживания.

Председатель:
Декан факультета
информационных технологий — д.пед.н., проф. Глазунова Е.Г.

Члены комиссии: д.т.н., проф. Лахно В.А.
д.ф.-м.н., проф. Малюков В.П.

ҚОСЫМША Б

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
Ғұмарбек Дәукеев атындағы АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ
БАСҚАРУ ЖҮЙЕЛЕРІ ЖӘНЕ АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ИНСТИТУТЫ

РЕСПУБЛИКА КАЗАХСТАН
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ имени Гумарбека Даукеева
НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
ИНСТИТУТ СИСТЕМ УПРАВЛЕНИЯ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

«БАСҚАРУ ЖҮЙЕЛЕРІ ЖӘНЕ АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР» ИНСТИТУТЫ

Адранова Асельхан Багдатовнаның диссертациялық

жұмысының нәтижелерін оқу процесіне енгізу туралы

АКТ

Комиссия құрамы:

Комиссия төрағасы - Алматы энергетика және байланыс университетінің «Басқару жүйелері және ақпараттық технологиялар» институтының директоры, PhD, профессор Т.С.Картбаев.

Комиссия мүшелері: IT – инжиниринг кафедрасының меңгерушісі, PhD, доцент А.А.Досжанова, IT – инжиниринг кафедрасының аға оқытушысы Ж.К.Алимсеитова.

Адранова Асельхан Багдатовнаның 6D060200 – «Информатика» мамандығы бойынша философия ғылымдарының докторы (PhD) дәрежесін алу үшін дайындаған «Қашықтықтан оқытудың ақпараттық қауіпсіздігін қамтамасыз етудің модельдері, әдістері және алгоритмдері» тақырыбындағы диссертациясының теориялық және эксперименттік зерттеулерін Алматы энергетика және байланыс университетінің «Басқару жүйелері және ақпараттық технологиялар» институтының IT – инжиниринг кафедрасының оқу процесінде сынақтан өткізу және енгізу үшін осы акт жасалып, төмендегі

нәтижелер оқу процесіне енгізілді және білім саласындағы 7М06102 – «Ақпараттық жүйелер» бойынша мамандарды даярлаудың оқу жоспарларына кіретін «Ақпаратты қорғау әдістері мен құралдары» пәнін оқыту кезінде қолданылады.

№	Енгізілетін жұмыстың атауы	Енгізу форма сы	Енгізу тиімділігі
1	Жоғары оқу орындарының қашықтықтан оқыту жүйесінің ақпараттық желілерінің кибер қатерін анықтау және оларды қорғау бойынша қарсышараларды таңдау әдісі	Дәріс	Білім алушыларды кешенді іздестіру, атап айтқанда, жаппай қызмет көрсету жүйесін қолдана отырып, қорғаушының ақпаратты қорғау құралдарын тиімді және ұтымды іздеу және ҚОЖ-нің ақпараттың құпиялылығына, тұтастығына және қол жетімділігіне деструктивті әсерлердің саны үнемі өсуі жағдайында сәйкес келетін қарсышараларды таңдау негізінде ҚОЖ-н қорғау әдістерімен және модельдерімен таныстыру болып табылады
2	Жаппай қызмет көрсету жүйесі ретінде қашықтықтан оқыту жүйесінің ақпараттық қауіпсіздікті басқару жүйесінің компьютерлік моделі	Зертха налық жұмыс	

Комисия төрағасы _____ Т.С.Картбаев

Комиссия мүшелері : _____ А.А.Досжанова

_____ Ж.К.Алимсеитова

ҚОСЫМША В

Справка

выдана докторанту по специальности 6D060200 – Информатика Адрановой Асельхан Багдатовне в том, что она действительно была исполнителем совместного проекта КазНПУ им.Абая с НИИ Высшая Школа Экономики (Россия, г.Москва) по теме «Мониторинг проникновения цифровых инструментов в учебный процесс вуза» (договор НИР № 19/04 от 19.04.2019).

и.о. директора Департамента науки
д.п.н., профессор У.М. Абдигапбарова

Справка

выдана докторанту по специальности 6D060200 – Информатика Адрановой Асельхан Багдатовне в том, что она действительно является исполнителем совместного проекта КазНПУ им.Абая с НИИ Высшая Школа Экономики (Россия, г.Москва) по теме Целевые и рамочные модели цифровой трансформации вузов: базовые направления и ключевые проекты (на примере Казахского национального педагогического университета имени Абая)» (договор НИР № 20/03 от 02.03.2020).

и.о. директора Департамента науки
д.п.н., профессор У.М. Абдигапбарова

ҚОСЫМША Г

1) ҚОЖ және оның АҚБЖ-нің әртүрлі жұмыс режимдерін ЖҚҚЖ ретінде модельдеуге арналған бағдарлама «ModelSMO2020» бағдарламалық өнімінің *m*-файлдар листингі

```
{модуль для проведения моделирования}
unit Zad1;
interface
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, ExtCtrls, StdCtrls,UnitGenerate,UnitKanal,UnitNakopitel, Vcl.ComCtrls;
type
  TFrZad1 = class(TForm)
    Button1: TButton;
    Label1: TLabel;
    Button2: TButton;
    GroupBox1: TGroupBox;
    GroupBox2: TGroupBox;
    RadioButton1: TRadioButton;
    RadioButton2: TRadioButton;
    Edit1: TEdit;
    GroupBox3: TGroupBox;
    Label2: TLabel;
    Label3: TLabel;
    Edit2: TEdit;
    Edit3: TEdit;
    GroupBox4: TGroupBox;
    Label4: TLabel;
    Edit4: TEdit;
    Label5: TLabel;
    Edit5: TEdit;
    Label6: TLabel;
    Edit6: TEdit;
    GroupBox5: TGroupBox;
    Label7: TLabel;
    Edit7: TEdit;
    CheckBox1: TCheckBox;
    GroupBox6: TGroupBox;
    CheckBox2: TCheckBox;
    CheckBox3: TCheckBox;
    CheckBox4: TCheckBox;
    CheckBox5: TCheckBox;
    CheckBox6: TCheckBox;
    CheckBox7: TCheckBox;
    StatusBar1: TStatusBar;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure FormClose(Sender: TObject; var Action: TCloseAction);
  end;
var
  FrZad1: TFrZad1;
```

```
  G:TGenerate;
  K:TKanal;
implementation
uses Zad1Statistica,Main;
{$R *.dfm}

// СТАРТ МОДЕЛИРОВАНИЯ
procedure TFrZad1.Button1Click(Sender: TObject);
var
i:byte;
p:real;
begin
FrZad1Statistica.Init;
FrZad1Statistica.Show;
FrZad1Statistica.Memo1.Clear;
GlobalTime:=0;
G:=TGenerate.Create;
G.Init('Источник_1',0,strtoint(Edit2.Text)-1,strtoint(Edit3.Text));
K:=TKanal.Create;
if CheckBox1.Checked then
 begin
  K.Init('Канал_1',strtoint(Edit4.Text),true,0,strtoint(Edit5.Text)-1,strtoint(Edit6.Text));
  K.N.Init('Накопитель_1',strtoint(Edit7.Text));
 end else K.Init('Канал_1',strtoint(Edit4.Text),false,0,strtoint(Edit5.Text)-1,strtoint(Edit6.Text));

FrZad1Statistica.Memo1.Lines.Add('ПАРАМЕТРЫ МОДЕЛИРОВАНИЯ');
if RadioButton1.Checked then FrZad1Statistica.Memo1.Lines.Add('Условие остановки модели:
Время='+Edit1.Text)
 else FrZad1Statistica.Memo1.Lines.Add('Условие остановки модели: Количество выполненных
заявок='+Edit1.Text);
FrZad1Statistica.Memo1.Lines.Add('Источник заявок: Время='+Edit2.Text+' Точность='+Edit3.Text);
if CheckBox1.Checked then FrZad1Statistica.Memo1.Lines.Add('Канал: Количество='+Edit4.Text+
                                ' Время='+Edit5.Text+' Точность='+
                                Edit6.Text+' Есть накопитель=да '+
                                'Емкость='+Edit7.Text) else
  FrZad1Statistica.Memo1.Lines.Add('Канал: Количество='+Edit4.Text+' Время='+Edit5.Text+' Точность='+
            Edit6.Text+' Есть накопитель=нет');
FrZad1Statistica.Memo1.Lines.Add('СТАРТ МОДЕЛИРОВАНИЯ!');

//---------------------------------------------------------------------------
repeat
if CheckBox2.Checked then FrZad1Statistica.Memo1.Lines.Add('Текущее время = '+inttostr(GlobalTime));
if G.Run then                    {=появление новой заявки=}
 begin
  if CheckBox3.Checked then
   begin
    FrZad1Statistica.Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Появление заявки.'+
    ' Всего создано заявок='+inttostr(G.AllCount)+
    ' Время след.заявки='+inttostr(G.NextTimeRun));
   end;
  FrZad1Statistica.Series1.AddXY(GlobalTime,0);
 end;
```

```
if G.Zayavka>0 then                    {=занятие канала=}
 begin
  K.ZayavkaIn(false);
  if (K.InKanal=false)and(K.InNakopitel=false) then
   begin
    G.ZayavkaOut(true);
    FrZad1Statistica.Series4.AddXY(GlobalTime,-1);
   end else G.ZayavkaOut(false);
 end else K.ZayavkaIn(true);

if CheckBox7.Checked and K.KanalFromNakopitel then
 begin
  FrZad1Statistica.Memo1.Lines.Add('='+inttostr(GlobalTime)+
  '= Заявка освободила накопитель. Количество заявок в накопителе='+
  inttostr(K.N.Emkost)+' Всего вышло заявок='+inttostr(K.N.ZayavkaRun));
 end;
if K.KanalFromNakopitel then
 begin
  FrZad1Statistica.Series3.AddXY(GlobalTime,2);
 end;
if CheckBox6.Checked and K.InNakopitel then
 begin
  FrZad1Statistica.Memo1.Lines.Add('='+inttostr(GlobalTime)+
  '= Заявка заняла накопитель. Количество заявок в накопителе='+
  inttostr(K.N.Emkost)+' Всего поступило заявок='+inttostr(K.N.AllCount));
 end;
if K.InNakopitel then
 begin
  FrZad1Statistica.Series2.AddXY(GlobalTime,1);
 end;
if CheckBox4.Checked and (K.InKanal or K.KanalFromNakopitel) then
 begin
  FrZad1Statistica.Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Занятие канала №'+
  inttostr(K.KanalNFree)+'. Всего поступило заявок='+inttostr(K.AllCount)+
  '. Время обсл.этой заявки='+inttostr(K.NextTimeRun[K.KanalNFree]));
 end;
if K.InKanal or K.KanalFromNakopitel then FrZad1Statistica.DownUpDown;

while K.Run do                         {=освобождение канала=}
 begin
  if CheckBox5.Checked then
   begin
    FrZad1Statistica.Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Освобождение канала №'+
    inttostr(K.KanalN)+'. Всего обслужено заявок='+inttostr(K.AllZayavkaRun));
   end;
  FrZad1Statistica.Down;
 end;
if K.ErrorLevel<>0 then
 begin
  FrZad1Statistica.Memo1.Lines.Add('ОШИБКА №'+inttostr(K.ErrorLevel));
  Button2Click(Sender);
 end;
```

```
inc(GlobalTime);
until (RadioButton1.Checked and(GlobalTime>strtoint(Edit1.Text)))OR
     (RadioButton2.Checked and(K.AllZayavkaRun>=strtoint(Edit1.Text)));
dec(GlobalTime);
FrZad1Statistica.EndDown;
//---------------------------------------------------------------------------
FrZad1Statistica.Memo1.Lines.Add('КОНЕЦ МОДЕЛИРОВАНИЯ!');
FrZad1Statistica.Memo1.Lines.Add('РЕЗУЛЬТАТЫ МОДЕЛИ');
FrZad1Statistica.Memo1.Lines.Add('Время работы модели: '+inttostr(GlobalTime));
FrZad1Statistica.Memo1.Lines.Add('Создано заявок: '+inttostr(G.AllCount));
FrZad1Statistica.Memo1.Lines.Add('Обслужено заявок: '+inttostr(K.AllZayavkaRun));
FrZad1Statistica.Memo1.Lines.Add('Потеряно заявок: '+inttostr(G.ZayavkaLoss));
for i:=1 to K.MaxKanal do
 begin
  if K.KanalCount[i]=0 then K.KanalTime[i]:=0;
  FrZad1Statistica.Memo1.Lines.Add('Время работы канала №'+inttostr(i)+': '+inttostr(K.KanalTime[i]));
  FrZad1Statistica.Memo1.Lines.Add('Поступило заявок в канал №'+inttostr(i)+': '+inttostr(K.KanalCount[i]));
  FrZad1Statistica.Memo1.Lines.Add('Обслужено заявок в канале №'+inttostr(i)+':
'+inttostr(K.ZayavkaRun[i]));
  p:=K.KanalTime[i]*100/GlobalTime;
  FrZad1Statistica.Memo1.Lines.Add('Коэффициент занятости канала №'+inttostr(i)+':
'+format('%4.1f',[p])+'%');
  FrZad1Statistica.Memo1.Lines.Add('Коэффициент простоя канала №'+inttostr(i)+': '+format('%4.1f',[100-
p])+'%');
 end;
if K.WithNakopitel then
 begin
  if K.N.ZayavkaRun<>0 then p:=K.N.AllTime/K.N.ZayavkaRun else p:=0;
  FrZad1Statistica.Memo1.Lines.Add('Среднее время пребывания заявки в накопителе:
'+format('%5.1f',[p]));
  FrZad1Statistica.Memo1.Lines.Add('Поступило заявок в накопитель: '+inttostr(K.N.AllCount));
  FrZad1Statistica.Memo1.Lines.Add('Число заявок поступивших на обслуживание в канал из накопителя:
'+
                        inttostr(K.N.ZayavkaRun));
  p:=K.N.AllTime*100/GlobalTime;
  FrZad1Statistica.Memo1.Lines.Add('Коэффициент занятости накопителя: '+format('%4.1f',[p])+'%');
  FrZad1Statistica.Memo1.Lines.Add('Коэффициент простоя накопителя: '+format('%4.1f',[100-p])+'%');
  FrZad1Statistica.Memo1.Lines.Add('Максимально заявок было в накопителе:
'+inttostr(K.N.EmkostMaximum));
 end;
end;
///
// ОСТАНОВКА МОДЕЛИРОВАНИЯ
procedure TFrZad1.Button2Click(Sender: TObject);
begin
RadioButton1.Checked:=true;
GlobalTime:=strtoint(Edit1.Text)+1;
FrZad1Statistica.Memo1.Lines.Add('ОСТАНОВКА МОДЕЛИРОВАНИЯ!');
end;
///
procedure TFrZad1.FormClose(Sender: TObject; var Action: TCloseAction);
begin
```

```
FrZad1.Destroy;
FrMain.N11.Enabled:=true;
FrMain.N21.Enabled:=true;
FrMain.N31.Enabled:=true;
end;
end.
{модуль для проведения моделирования}
unit Zad3;
interface
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, ExtCtrls, StdCtrls,UnitGenerate,UnitKanal,UnitNakopitel, Vcl.ComCtrls;
type
  TFrZad3 = class(TForm)
    Button1: TButton;
    Label1: TLabel;
    Button2: TButton;
    GroupBox1: TGroupBox;
    GroupBox3: TGroupBox;
    Label2: TLabel;
    Label3: TLabel;
    Edit2: TEdit;
    Edit3: TEdit;
    GroupBox4: TGroupBox;
    Label5: TLabel;
    Edit5: TEdit;
    Label6: TLabel;
    Edit6: TEdit;
    GroupBox5: TGroupBox;
    Label7: TLabel;
    Edit7: TEdit;
    CheckBox1: TCheckBox;
    GroupBox6: TGroupBox;
    CheckBox2: TCheckBox;
    CheckBox3: TCheckBox;
    CheckBox4: TCheckBox;
    CheckBox5: TCheckBox;
    CheckBox6: TCheckBox;
    CheckBox7: TCheckBox;
    ComboBox1: TComboBox;
    ComboBox3: TComboBox;
    CheckBox9: TCheckBox;
    GroupBox2: TGroupBox;
    RadioButton1: TRadioButton;
    RadioButton2: TRadioButton;
    Edit1: TEdit;
    StatusBar1: TStatusBar;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure FormClose(Sender: TObject; var Action: TCloseAction);
  end;
var
```

```
  FrZad3: TFrZad3;
  G1:TGenerate;                  // источник заявок
  K1:TKanal;                     // канал
implementation
uses Zad3Statistica, Main;
{$R *.dfm}
// СТАРТ МОДЕЛИРОВАНИЯ
procedure TFrZad3.Button1Click(Sender: TObject);
var
i:byte;
p:real;
begin
FrZad3Statistica.Init;
FrZad3Statistica.Show;
FrZad3Statistica.Memo1.Clear;
GlobalTime:=0;
G1:=TGenerate.Create;
G1.Init('Источник_1',ComboBox1.ItemIndex,strtoint(Edit2.Text)-1,strtoint(Edit3.Text));
K1:=TKanal.Create;
if CheckBox1.Checked then
 begin
  K1.Init('Канал_1',1,true,ComboBox3.ItemIndex,strtoint(Edit5.Text)-1,strtoint(Edit6.Text));
  K1.N.Init('Накопитель_1',strtoint(Edit7.Text));
 end else
 begin
  K1.Init('Канал_1',1,false,ComboBox3.ItemIndex,strtoint(Edit5.Text)-1,strtoint(Edit6.Text));
 end;
FrZad3Statistica.Memo1.Lines.Add('ПАРАМЕТРЫ МОДЕЛИРОВАНИЯ');
if RadioButton1.Checked then FrZad3Statistica.Memo1.Lines.Add('Условие остановки модели:
Время='+Edit1.Text)
 else FrZad3Statistica.Memo1.Lines.Add('Условие остановки модели: Количество выполненных
заявок='+Edit1.Text);
FrZad3Statistica.Memo1.Lines.Add('Источник заявок: Время='+Edit2.Text+' Точность='+Edit3.Text+'
'+ComboBox1.Text);
FrZad3Statistica.Memo1.Lines.Add('Канал:');
if CheckBox1.Checked then FrZad3Statistica.Memo1.Lines.Add('Есть накопитель №1=да  Емкость для
накопителя 1 ='+Edit7.Text)
 else FrZad3Statistica.Memo1.Lines.Add('Есть накопитель=нет');
FrZad3Statistica.Memo1.Lines.Add('Время обработки ='+Edit5.Text+' Точность='+Edit6.Text+'
'+ComboBox3.Text);
FrZad3Statistica.Memo1.Lines.Add('СТАРТ МОДЕЛИРОВАНИЯ!');

//---------------------------------------------------------------------------
repeat
if CheckBox2.Checked then FrZad3Statistica.Memo1.Lines.Add('Текущее время = '+inttostr(GlobalTime));
G1.Run;

if G1.Zayavka>0 then
 begin                    {----заявка от источника -----}
  FrZad3Statistica.SetInfo(1);
  K1.ZayavkaIn(false);          // заявка пробует занять канал
  if (K1.InKanal=false)and(K1.InNakopitel=false) then
```

```
   begin                        // заявка не заняла канал или накопитель
    G1.ZayavkaOut(true);          // потеря заявки
    FrZad3Statistica.SetInfo(8);
   end else
   begin                        // заявка заняла канал
    G1.ZayavkaOut(false);         // заявка не потеряна
    if K1.InKanal then
     begin                      // заявка заняла канал от источника
      FrZad3Statistica.SetInfo(11);
     end;
    if K1.KanalFromNakopitel then
     begin                        // заявка заняла канал из накопителя
      FrZad3Statistica.SetInfo(5);
      FrZad3Statistica.SetInfo(11);
     end;
    if K1.InNakopitel then FrZad3Statistica.SetInfo(4);  // заявка заняла накопитель
   end;
 end else
 begin                        {----нет заявки от источника 1-----}
  K1.ZayavkaIn(true);           {заявка может попасть из накопителя}
  if K1.KanalFromNakopitel then
   begin                        // заявка заняла канал из накопителя
    FrZad3Statistica.SetInfo(5);
    FrZad3Statistica.SetInfo(11);
   end;
 end;
if K1.Run then                    // Заявка от источника 1 выполнена
 begin
  FrZad3Statistica.SetInfo(12);
  FrZad3Statistica.SetInfo(10);
 end;
if K1.ErrorLevel<>0 then
 begin
  FrZad3Statistica.Memo1.Lines.Add('ОШИБКА №'+inttostr(K1.ErrorLevel));
  Button2Click(Sender);
 end;
inc(GlobalTime);
until (RadioButton1.Checked and(GlobalTime>strtoint(Edit1.Text)))OR
     (RadioButton2.Checked and(K1.AllZayavkaRun>=strtoint(Edit1.Text)));
FrZad3Statistica.SetInfo(15);
dec(GlobalTime);

//---------------------------------------------------------------------------
with FrZad3Statistica.Memo1.Lines do
begin
 Add('КОНЕЦ МОДЕЛИРОВАНИЯ!');
 Add('РЕЗУЛЬТАТЫ МОДЕЛИ');
 Add('Время работы модели: '+inttostr(GlobalTime));
 Add('Создано заявок: '+inttostr(G1.AllCount));
 Add('Обслужено заявок: '+inttostr(K1.AllZayavkaRun));
 Add('Потеряно заявок: '+inttostr(G1.ZayavkaLoss));
```

```
 Add('Время работы канала: '+inttostr(K1.KanalTime[1]));
 Add('Поступило заявок в канал: '+inttostr(K1.KanalCount[1]));
 Add('Обслужено заявок в канале: '+inttostr(K1.ZayavkaRun[1]));
 p:=K1.KanalTime[1]*100/GlobalTime;
 Add('Коэффициент занятости канала: '+format('%4.1f',[p])+'%');
 Add('Коэффициент простоя канала: '+format('%4.1f',[100-p])+'%');

if K1.WithNakopitel then
 begin
  if K1.N.ZayavkaRun<>0 then p:=K1.N.AllTime/K1.N.ZayavkaRun else p:=0;
  Add('Среднее время пребывания заявки в накопителе: '+format('%5.1f',[p]));
  Add('Поступило заявок в накопитель: '+inttostr(K1.N.AllCount));
  Add('Число заявок поступивших на обслуживание в канал из накопителя: '+
                        inttostr(K1.N.ZayavkaRun));
  p:=K1.N.AllTime*100/GlobalTime;
  Add('Коэффициент занятости накопителя: '+format('%4.1f',[p])+'%');
  Add('Коэффициент простоя накопителя: '+format('%4.1f',[100-p])+'%');
  Add('Максимально заявок было в накопителе: '+inttostr(K1.N.EmkostMaximum));
 end;
end;  // end with
end;
///
// ОСТАНОВКА МОДЕЛИРОВАНИЯ
procedure TFrZad3.Button2Click(Sender: TObject);
begin
RadioButton1.Checked:=true;
GlobalTime:=strtoint(Edit1.Text)+1;
FrZad3Statistica.Memo1.Lines.Add('ОСТАНОВКА МОДЕЛИРОВАНИЯ!');
end;
///
procedure TFrZad3.FormClose(Sender: TObject; var Action: TCloseAction);
begin
FrZad3.Destroy;
FrMain.N11.Enabled:=true;
FrMain.N21.Enabled:=true;
FrMain.N31.Enabled:=true;
end;
end.{модуль вывода информации о ходе моделирования}
unit Zad1Statistica;
interface
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, Series, TeEngine, ExtCtrls, TeeProcs, Chart, StdCtrls,
  VclTee.TeeGDIPlus;
type
  TFrZad1Statistica = class(TForm)
    Memo1: TMemo;
    Label1: TLabel;
    Chart1: TChart;
    Series1: TPointSeries;
    Series2: TPointSeries;
    Series3: TPointSeries;
```

```
    Series5: TLineSeries;
    Series6: TLineSeries;
    Series4: TPointSeries;
    Series7: TLineSeries;
    ScrollBox1: TScrollBox;
    Label2: TLabel;
    Memo2: TMemo;
    Label3: TLabel;
    Edit1: TEdit;
    Label4: TLabel;
    Edit2: TEdit;
    Button1: TButton;
    Series8: TLineSeries;
    Series9: TLineSeries;
    Series10: TLineSeries;
    Series11: TLineSeries;
    PROCEDURE Init;
    PROCEDURE DownUpDown;
    PROCEDURE Down;
    PROCEDURE EndDown;
    procedure FormActivate(Sender: TObject);
    procedure Button1Click(Sender: TObject);
  end;
var
  FrZad1Statistica: TFrZad1Statistica;
implementation
uses Main, Zad1;
var
max_time:longint;
{$R *.dfm}
// НАЧАЛЬНЫЕ ЗНАЧЕНИЯ ДЛЯ ПОСТРОЕНИЯ ДИАГРАММЫ
PROCEDURE TFrZad1Statistica.Init;
var
i:byte;
BEGIN
Chart1.RemoveAllSeries;
Series1.Clear;
Chart1.AddSeries(FrZad1Statistica.Series1);
Series2.Clear;
Chart1.AddSeries(FrZad1Statistica.Series2);
Series3.Clear;
Chart1.AddSeries(FrZad1Statistica.Series3);
Series4.Clear;
Chart1.AddSeries(FrZad1Statistica.Series4);

for i:=5 to 4+strtoint(FrZad1.Edit4.Text) do
 begin
  with TLineSeries(FindComponent('Series'+inttostr(i)))do
  begin
   Clear;
   AddXY(0,2*(i-4)+1);
  end;
```

```
  Chart1.AddSeries(TLineSeries(FindComponent('Series'+inttostr(i))));
 end;
max_time:=0;
END;
///
// ставит 4 точки: канал свободен, канал занят, канал свободен
PROCEDURE TFrZad1Statistica.DownUpDown;
var
i:byte;
BEGIN
with TLineSeries(FindComponent('Series'+inttostr(4+K.KanalNFree)))do
begin
AddXY(GlobalTime,2*K.KanalNFree+1);
AddXY(GlobalTime,2*K.KanalNFree+2);
AddXY(K.NextTimeRun[K.KanalNFree],2*K.KanalNFree+2);
AddXY(K.NextTimeRun[K.KanalNFree],2*K.KanalNFree+1);
if max_time<K.NextTimeRun[K.KanalNFree] then max_time:=K.NextTimeRun[K.KanalNFree];
end;
END;
///
// ставит точку: канал свободен
PROCEDURE TFrZad1Statistica.Down;
var
i:byte;
BEGIN
with TLineSeries(FindComponent('Series'+inttostr(4+K.KanalN)))do
 AddXY(GlobalTime,2*K.KanalN+1);
END;
///
// после завершения моделирования ставит точку: канал свободен
PROCEDURE TFrZad1Statistica.EndDown;
var
i:byte;
BEGIN
Memo2.Clear;
Memo2.Lines.Add('Ось X: время');
Memo2.Lines.Add('Ось Y: состояние объектов модели');
if G.ZayavkaLoss>0 then Memo2.Lines.Add('-1 = Потеря заявки');
Memo2.Lines.Add(' 0 = Появление заявки');
Memo2.Lines.Add(' 1 = Заявка заняла накопитель');
Memo2.Lines.Add(' 2 = Заявка освободила накопитель');

for i:=5 to 4+strtoint(FrZad1.Edit4.Text) do
if K.KanalCount[i-4]>0 then
 begin
  with TLineSeries(FindComponent('Series'+inttostr(i)))do AddXY(max_time,2*(i-4)+1);
  Memo2.Lines.Add(' '+inttostr((i-4)*2+1)+' = Канал №'+inttostr(i-4)+' свободен');
  Memo2.Lines.Add(' '+inttostr((i-4)*2+2)+' = Канал №'+inttostr(i-4)+' занят');
 end;
END;
///
// активизация формы
```

```
procedure TFrZad1Statistica.FormActivate(Sender: TObject);
begin
Edit1.Text:='406';
Edit2.Text:='876';
Button1Click(Sender);
end;
///
// изменение размеров диаграммы
procedure TFrZad1Statistica.Button1Click(Sender: TObject);
begin
Chart1.Height:=strtoint(Edit1.Text);
Chart1.Width:=strtoint(Edit2.Text);
end;
///
end.
{модуль вывода информации о ходе моделирования}
unit Zad2Statistica;
interface
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, Series, TeEngine, ExtCtrls, TeeProcs, Chart, StdCtrls,
  VclTee.TeeGDIPlus;
type
  TFrZad2Statistica = class(TForm)
    Memo1: TMemo;
    Label1: TLabel;
    Chart1: TChart;
    ScrollBox1: TScrollBox;
    Label2: TLabel;
    Memo2: TMemo;
    Label3: TLabel;
    Edit1: TEdit;
    Label4: TLabel;
    Edit2: TEdit;
    Button1: TButton;
    Series1: TPointSeries;
    Series2: TPointSeries;
    Series3: TPointSeries;
    Series4: TPointSeries;
    Series5: TLineSeries;
    Series6: TPointSeries;
    Series7: TPointSeries;
    Series8: TPointSeries;
    Series9: TPointSeries;
    PROCEDURE Init;
    PROCEDURE SetInfo(const Info:integer);
    procedure FormActivate(Sender: TObject);
    procedure Button1Click(Sender: TObject);
  end;
var
  FrZad2Statistica: TFrZad2Statistica;
implementation
```

```
uses Main, Zad2;
var
max_time:longint;
{$R *.dfm}
// НАЧАЛЬНЫЕ ЗНАЧЕНИЯ ДЛЯ ПОСТРОЕНИЯ ДИАГРАММЫ
PROCEDURE TFrZad2Statistica.Init;
BEGIN
Chart1.RemoveAllSeries;
Series1.Clear;
Chart1.AddSeries(FrZad2Statistica.Series1);
Series2.Clear;
Chart1.AddSeries(FrZad2Statistica.Series2);
Series3.Clear;
Chart1.AddSeries(FrZad2Statistica.Series3);
Series4.Clear;
Chart1.AddSeries(FrZad2Statistica.Series4);
Series5.Clear;
Chart1.AddSeries(FrZad2Statistica.Series5);
Series6.Clear;
Chart1.AddSeries(FrZad2Statistica.Series6);
Series7.Clear;
Chart1.AddSeries(FrZad2Statistica.Series7);
Series8.Clear;
Chart1.AddSeries(FrZad2Statistica.Series8);
Series9.Clear;
Chart1.AddSeries(FrZad2Statistica.Series9);

Memo2.Clear;
Memo2.Lines.Add('Ось X: время');
Memo2.Lines.Add('Ось Y: состояние объектов модели');
Memo2.Lines.Add('-1 = Потеря заявки');
Memo2.Lines.Add(' 0 = Появление заявки от источника №1');
Memo2.Lines.Add(' 2 = Заявка заняла накопитель №1');
Memo2.Lines.Add(' 3 = Заявка освободила накопитель №1');
Memo2.Lines.Add(' 5 = Канал свободен');
Memo2.Lines.Add(' 6 = Канал выполняет заявку от источника №1');
Memo2.Lines.Add(' 7 = Канал выполняет заявку от источника №2');
Memo2.Lines.Add(' 9 = Заявка освободила накопитель №2');
Memo2.Lines.Add(' 10 = Заявка заняла накопитель №2');
Memo2.Lines.Add(' 12 = Появление заявки от источника №2');
Memo2.Lines.Add(' Крест - выполнение заявки прервано');
END;
///

// Показывает информацию по параметру
PROCEDURE TFrZad2Statistica.SetInfo(const Info:integer);
BEGIN
case Info of
0: begin              // создана заявка от источника 2
   if FrZad2.CheckBox3.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Появление заявки от источника 2.'+
                ' Всего создано заявок='+inttostr(G2.AllCount)+
```

```
                ' Время след.заявки='+inttostr(G2.NextTimeRun));
    Series2.AddXY(GlobalTime,0);
   end;
 1: begin              // создана заявка от источника 1
    if FrZad2.CheckBox3.Checked then
     Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Появление заявки от источника 1.'+
                ' Всего создано заявок='+inttostr(G1.AllCount)+
                ' Время след.заявки='+inttostr(G1.NextTimeRun));
    Series2.AddXY(GlobalTime,12);
   end;
 2: begin              // заявка заняла накопитель 2
    if FrZad2.CheckBox6.Checked then
     Memo1.Lines.Add('='+inttostr(GlobalTime)+
      '= Заявка заняла накопитель 2. Количество заявок в накопителе='+
      inttostr(K2.N.Emkost)+' Всего поступило заявок='+inttostr(K2.N.AllCount));
    Series3.AddXY(GlobalTime,2);
   end;
 3: begin              // заявка освободила накопитель 2
    if FrZad2.CheckBox7.Checked then
     Memo1.Lines.Add('='+inttostr(GlobalTime)+
     '= Заявка освободила накопитель 2. Количество заявок в накопителе='+
     inttostr(K2.N.Emkost)+' Всего вышло заявок='+inttostr(K2.N.ZayavkaRun));
    Series4.AddXY(GlobalTime,3);
   end;
 4: begin              // заявка заняла накопитель 1
    if FrZad2.CheckBox6.Checked then
     Memo1.Lines.Add('='+inttostr(GlobalTime)+
      '= Заявка заняла накопитель 1. Количество заявок в накопителе='+
      inttostr(K1.N.Emkost)+' Всего поступило заявок='+inttostr(K1.N.AllCount));
    Series7.AddXY(GlobalTime,10);
   end;
 5: begin              // заявка освободила накопитель 1
    if FrZad2.CheckBox7.Checked then
     Memo1.Lines.Add('='+inttostr(GlobalTime)+
     '= Заявка освободила накопитель 1. Количество заявок в накопителе='+
     inttostr(K1.N.Emkost)+' Всего вышло заявок='+inttostr(K1.N.ZayavkaRun));
    Series6.AddXY(GlobalTime,9);
   end;
 6: begin              // потеря заявки от источника 2
    if FrZad2.CheckBox9.Checked then
     Memo1.Lines.Add('='+inttostr(GlobalTime)+
     '= Потеря заявки от источника 2. Всего потеряно заявок='+inttostr(G2.ZayavkaLoss));
    Series1.AddXY(GlobalTime,-1);
   end;
 7: begin              // заявка от источника 2 заняла канал
    if FrZad2.CheckBox4.Checked then
     Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Заявка от источника 2 заняла канал.'+
     ' Всего поступило заявок от источника 2='+inttostr(K2.AllCount)+
     ' Время обсл.этой заявки='+inttostr(K2.NextTimeRun[K2.KanalNFree]));
    Series5.AddXY(GlobalTime,5);
    Series5.AddXY(GlobalTime,7);
   end;
```

```
8: begin              // потеря заявки от источника 1
   if FrZad2.CheckBox9.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+
    '= Потеря заявки от источника 1. Всего потеряно заявок='+inttostr(G1.ZayavkaLoss));
   Series1.AddXY(GlobalTime,-1);
  end;
9: begin              // заявка прервана
   if FrZad2.CheckBox11.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+
    '= Выполнение заявки прервано. Всего прервано заявок='+inttostr(ZayavkaPrervana));
   Series9.AddXY(GlobalTime,6);
  end;
10:begin              // заявка освобождает канал 1
   if FrZad2.CheckBox5.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Заявка от источника 1 освобождает канал.');
   Series5.AddXY(GlobalTime,6);
   Series5.AddXY(GlobalTime,5);
  end;
11:begin              // зявка от источника 1 заняла канал
   if FrZad2.CheckBox4.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Заявка от источника 1 заняла канал.'+
    ' Всего поступило заявок от источника 1='+inttostr(K1.AllCount)+
    ' Время обсл.этой заявки='+inttostr(K1.NextTimeRun[K1.KanalNFree]));
   Series5.AddXY(GlobalTime,5);
   Series5.AddXY(GlobalTime,6);
  end;
12:begin              // зявка от источника 1 выполнена
   if FrZad2.CheckBox5.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Заявка от источника 1 выполнена.'+
    ' Всего обслужено заявок='+inttostr(K1.AllZayavkaRun));
  end;
13:begin              // зявка от источника 2 выполнена
   if FrZad2.CheckBox5.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Заявка от источника 2 выполнена.'+
    ' Всего обслужено заявок='+inttostr(K2.AllZayavkaRun));
  end;
14:begin              // заявка освобождает канал 2
   if FrZad2.CheckBox5.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Заявка от источника 2 освобождает канал.');
   Series5.AddXY(GlobalTime,7);
   Series5.AddXY(GlobalTime,5);
  end;
15:begin              // Конец - дорисовать линию
   if (K1.RunParam=0)and(K2.RunParam=0) then Series5.AddXY(GlobalTime,5) else
   if (K2.RunParam=0) then Series5.AddXY(GlobalTime,6) else
   if (K1.RunParam=0) then Series5.AddXY(GlobalTime,7);
  end;
end;  // end case
END;
///
// активизация формы
procedure TFrZad2Statistica.FormActivate(Sender: TObject);
```

```
begin
Edit1.Text:='406';
Edit2.Text:='876';
Button1Click(Sender);
end;
///
// изменение размеров диаграммы
procedure TFrZad2Statistica.Button1Click(Sender: TObject);
begin
Chart1.Height:=strtoint(Edit1.Text);
Chart1.Width:=strtoint(Edit2.Text);
end;
///
End.{модуль вывода информации о ходе моделирования}
unit Zad3Statistica;
interface
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, Series, TeEngine, ExtCtrls, TeeProcs, Chart, StdCtrls,
  VclTee.TeeGDIPlus;
type
  TFrZad3Statistica = class(TForm)
    Memo1: TMemo;
    Label1: TLabel;
    Chart1: TChart;
    ScrollBox1: TScrollBox;
    Label2: TLabel;
    Memo2: TMemo;
    Label3: TLabel;
    Edit1: TEdit;
    Label4: TLabel;
    Edit2: TEdit;
    Button1: TButton;
    Series1: TPointSeries;
    Series2: TPointSeries;
    Series3: TPointSeries;
    Series4: TPointSeries;
    Series5: TLineSeries;
    PROCEDURE Init;
    PROCEDURE SetInfo(const Info:integer);
    procedure FormActivate(Sender: TObject);
    procedure Button1Click(Sender: TObject);
  end;
var
  FrZad3Statistica: TFrZad3Statistica;
implementation
uses Main, Zad3;
var
max_time:longint;
{$R *.dfm}
// НАЧАЛЬНЫЕ ЗНАЧЕНИЯ ДЛЯ ПОСТРОЕНИЯ ДИАГРАММЫ
PROCEDURE TFrZad3Statistica.Init;
```

```
BEGIN
Chart1.RemoveAllSeries;
Series1.Clear;
Chart1.AddSeries(Series1);
Series2.Clear;
Chart1.AddSeries(Series2);
Series3.Clear;
Chart1.AddSeries(Series3);
Series4.Clear;
Chart1.AddSeries(Series4);
Series5.Clear;
Chart1.AddSeries(Series5);

Memo2.Clear;
Memo2.Lines.Add('Ось X: время');
Memo2.Lines.Add('Ось Y: состояние объектов модели');
Memo2.Lines.Add('-1 = Потеря заявки');
Memo2.Lines.Add(' 0 = Появление заявки от источника');
Memo2.Lines.Add(' 1 = Заявка заняла накопитель');
Memo2.Lines.Add(' 2 = Заявка освободила накопитель');
Memo2.Lines.Add(' 3 = Канал свободен');
Memo2.Lines.Add(' 4 = Канал выполняет заявку');
END;
///
// Показывает информацию по параметру
PROCEDURE TFrZad3Statistica.SetInfo(const Info:integer);
BEGIN
case Info of
1: begin              // создана заявка от источника 1
   if FrZad3.CheckBox3.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Появление заявки от источника.'+
                ' Всего создано заявок='+inttostr(G1.AllCount)+
                ' Время след.заявки='+inttostr(G1.NextTimeRun));
   Series2.AddXY(GlobalTime,0);
  end;
4: begin              // заявка заняла накопитель 1
   if FrZad3.CheckBox6.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+
     '= Заявка заняла накопитель. Количество заявок в накопителе='+
     inttostr(K1.N.Emkost)+' Всего поступило заявок='+inttostr(K1.N.AllCount));
   Series3.AddXY(GlobalTime,1);
  end;
5: begin              // заявка освободила накопитель 1
   if FrZad3.CheckBox7.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+
    '= Заявка освободила накопитель 1. Количество заявок в накопителе='+
    inttostr(K1.N.Emkost)+' Всего вышло заявок='+inttostr(K1.N.ZayavkaRun));
   Series4.AddXY(GlobalTime,2);
  end;
8: begin              // потеря заявки от источника 1
   if FrZad3.CheckBox9.Checked then
    Memo1.Lines.Add('='+inttostr(GlobalTime)+
```

```
    '= Потеря заявки. Всего потеряно заявок='+inttostr(G1.ZayavkaLoss));
    Series1.AddXY(GlobalTime,-1);
   end;
10:begin              // заявка освобождает канал 1
    if FrZad3.CheckBox5.Checked then
     Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Заявка освобождает канал.');
    Series5.AddXY(GlobalTime,4);
    Series5.AddXY(GlobalTime,3);
   end;
11:begin              // зявка от источника 1 заняла канал
    if FrZad3.CheckBox4.Checked then
     Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Заявка заняла канал.'+
     ' Всего поступило заявок='+inttostr(K1.AllCount)+
     ' Время обсл.этой заявки='+inttostr(K1.NextTimeRun[K1.KanalNFree]));
    Series5.AddXY(GlobalTime,3);
    Series5.AddXY(GlobalTime,4);
   end;
12:begin              // зявка от источника 1 выполнена
    if FrZad3.CheckBox5.Checked then
     Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Заявка выполнена.'+
     ' Всего обслужено заявок='+inttostr(K1.AllZayavkaRun));
   end;
15:begin              // Конец - дорисовать линию
    if K1.RunParam=0 then Series5.AddXY(GlobalTime,3) else Series5.AddXY(GlobalTime,4);
   end;
end;  // end case
END;
///
// активизация формы
procedure TFrZad3Statistica.FormActivate(Sender: TObject);
begin
Edit1.Text:='406';
Edit2.Text:='876';
Button1Click(Sender);
end;
///
// изменение размеров диаграммы
procedure TFrZad3Statistica.Button1Click(Sender: TObject);
begin
Chart1.Height:=strtoint(Edit1.Text);
Chart1.Width:=strtoint(Edit2.Text);
end;
///
end.
unit Main;
interface
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls, Menus,UnitGenerate,UnitKanal,UnitNakopitel;
type
  TFrMain = class(TForm)
    MainMenu1: TMainMenu;
```

```
    N11: TMenuItem;
    N21: TMenuItem;
    N31: TMenuItem;
    procedure N11Click(Sender: TObject);
    procedure N21Click(Sender: TObject);
    procedure N31Click(Sender: TObject);
    procedure N1Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;
var
  FrMain: TFrMain;
  GlobalTime:longint;              // время модели
  function Normal(const Mx, Sigma: Extended): Extended;
  function Exponent(const LeftGr, T: Extended): Extended;
implementation
uses Zad1,Zad2,Zad3;
{$R *.dfm}
// Возвращает случайное число, распределенное по нормальному закону распределения
// с заданным математическим ожиданием и дисперсией
{ Mx:=(a+b)/2;  Sigma:=(b-a)/2*sqrt(3); }
function Normal(const Mx, Sigma: Extended): Extended;
var
  a, b, r, Sq: Extended;
begin
  repeat
    a := 2*Random - 1;
    b := 2*Random - 1;
    r := Sqr(a) + Sqr(b);
  until r<1;
  Sq := Sqrt(-2*Ln(r)/r);
  Result := Mx + Sigma * a * Sq;
end; //Возвращает случайное число, распределенное по экспоненциальному закону распределения
// LeftGr - левая граница интервала  T - точность *2
// возвращает число в интервале [LeftGr, LeftGr+T]
{f(x)=a*e^(-a*x) }
function Exponent(const LeftGr, T: Extended): Extended;
begin
Result:=LeftGr+T*exp(-T*random);
end;
///
procedure TFrMain.N11Click(Sender: TObject);
begin
FrMain.N11.Enabled:=false;
FrMain.N21.Enabled:=false;
FrMain.N31.Enabled:=false;
FrMain.Height:=330;
FrMain.Width:=690;
Application.CreateForm(TFrZad1, FrZad1);
end;
```

```
procedure TFrMain.N21Click(Sender: TObject);
begin
FrMain.N11.Enabled:=false;
FrMain.N21.Enabled:=false;
FrMain.N31.Enabled:=false;
FrMain.Height:=507;
FrMain.Width:=775;
Application.CreateForm(TFrZad2, FrZad2);
end;
procedure TFrMain.N31Click(Sender: TObject);
begin
FrMain.N11.Enabled:=false;
FrMain.N21.Enabled:=false;
FrMain.N31.Enabled:=false;
FrMain.Height:=336;
FrMain.Width:=895;
Application.CreateForm(TFrZad3, FrZad3);
end;
procedure TFrMain.N1Click(Sender: TObject);
begin
//winhelp(FrMain.Handle,'Help.hlp',HELP_CONTEXT,0);
end;
end.
{модуль выполняющий функции ИСТОЧНИКА ЗАЯВОК}
unit UnitGenerate;
interface
type
  TGenerate = class
  Name:string;                  // имя объекта
  Zakon:byte;                   // закон распределения сл.чисел
  a,b:integer;                  // интервал сл.чисел
  Mx,Sigma:real;                // мат.ожидание и дисперсия
  AllTime,AllCount:longint;       // общее время работы объекта и кол. созданных заявок
  NextTimeRun:longint;            // след.время появления заявки
  Zayavka,ZayavkaLoss:longint;     // Zayavka>0 если создана заявка; Кол. потерянных заявок
  PROCEDURE Init(const AName:string;AZakon:byte;ATime,AdxTime:integer);
  FUNCTION Run:boolean;
  PROCEDURE SetNextTime;
  PROCEDURE ZayavkaOut(const Loss:boolean);
  end;
implementation
uses main;
// ИНИЦИАЛИЗАЦИЯ
PROCEDURE TGenerate.Init(const AName:string;AZakon:byte;ATime,AdxTime:integer);
BEGIN
Name:=AName;
Zakon:=AZakon;
case Zakon of
0: begin              // равномерный закон распределения чисел в интервале [a,b]
   a:=ATime-AdxTime;
   b:=ATime+AdxTime;
   Mx:=(a+b)/2;
```

```
   Sigma:=(b-a)/2*sqrt(3);
  end;
1: begin              // экспоненциальный закон распределения чисел в интервале [a,b]
   Sigma:=AdxTime*2;
   a:=ATime-AdxTime;
   b:=ATime+AdxTime;
   Mx:=ATime;
  end;
end;  // end case
AllTime:=0;
AllCount:=0;
NextTimeRun:=0;
Zayavka:=0;
ZayavkaLoss:=0;
END;
///

// ВЫПОНИТЬ
{алгоритм
0. Статистика времени работы
1. Проверить время, если время пришло, тогда
2. Получить следующее время
3. Создать заявку}
FUNCTION TGenerate.Run:boolean;
BEGIN
{0.}
inc(AllTime);
{1.}
Run:=false;
if (GlobalTime=NextTimeRun)or(NextTimeRun=0) then
 begin
  Run:=true;
  {2.}
  SetNextTime;
  {3.}
  inc(Zayavka);
  inc(AllCount);
 end;
END;
//
// УСТАНОВКА СЛЕДУЮЩЕГО МОМЕНТА ВЫПОЛНЕНИЯ
PROCEDURE TGenerate.SetNextTime;
BEGIN
repeat
case Zakon of
0: NextTimeRun:=round(Normal(Mx,Sigma));
1: NextTimeRun:=round(Exponent(Mx,Sigma));
end;  // end case
until (NextTimeRun>=a)and(NextTimeRun<=b);
NextTimeRun:=NextTimeRun+GlobalTime+1;
END;
///
```

```
// УХОД ЗАЯВКИ ИЗ ИСТОЧНИКА
{Loss=true если заявка была потеряна}
PROCEDURE TGenerate.ZayavkaOut(const Loss:boolean);
BEGIN
if Zayavka-1<0 then exit;
dec(Zayavka);
if Loss then inc(ZayavkaLoss);
END;
///
end.
{модуль выполняющий функции КАНАЛА ОБСЛУЖИВАНИЯ}
unit UnitKanal;
interface
uses UnitNakopitel;
type
  TKanal = class
  Name:string;                  // имя объекта
  Zakon:byte;                   // закон распределения сл.чисел
  a,b:integer;                  // интервал сл.чисел
  Mx,Sigma:real;                // мат.ожидание и дисперсия
  AllTime,AllCount,             // время работы, всего пришло заявок,
  AllZayavkaRun:longint;        // выполнено заявок
  KanalTime,KanalCount,         // время работы i-го канала, всего пришло заявок,
  ZayavkaRun:array[1..255]of longint;  // выполнено заявок в канале i
  WithNakopitel:boolean;        // true если канал с накопителем
  NextTimeRun:array[1..255]of longint; // время завершения i-й заявки
  KanalStatus:array[1..255]of boolean; // false-канал свободен
  Kanal:byte;                   // число занятых каналов
  MaxKanal:byte;                // максимально возможно каналов
  RunParam:byte;                // 0-канал полностью свободен
                                // 1-канал работает, есть место для следуюжей заявки
                                // 2-канал полностью занят, нет места для следуюжей заявки
  KanalN,KanalNFree:byte;       // номер освободившегося канала, номер занятого канала
  N:TNakopitel;                 // накопитель для канала
  KanalFromNakopitel,InNakopitel:boolean; // true-заявка поступила в канал из накопителя
                                // true-заявка поступила в накопитель
  InKanal:boolean;              // true-заявка поступила в канал из-вне
  ErrorLevel:byte;              // 0-нет ошибок
  PROCEDURE Init(const AName:string;AMaxKanal:longint;AWithNakopitel:boolean;
            AZakon:byte;ATime,AdxTime:integer);
  FUNCTION Run:boolean;
  FUNCTION GetFreeKanal:byte;
  PROCEDURE SetNextTime;
  PROCEDURE ZayavkaIn(const FromNakopitel:boolean);
  PROCEDURE ZayavkaOut;
  end;
implementation
uses main,SysUtils;
var
i:byte;
// ИНИЦИАЛИЗАЦИЯ
PROCEDURE TKanal.Init(const AName:string;AMaxKanal:longint;AWithNakopitel:boolean;
```

```
                AZakon:byte;ATime,AdxTime:integer);
BEGIN
Name:=AName;
MaxKanal:=AMaxKanal;
WithNakopitel:=AWithNakopitel;
if WithNakopitel then N:=TNakopitel.Create;
Zakon:=AZakon;
case Zakon of
0: begin              // равномерный закон распределения чисел в интервале [a,b]
    a:=ATime-AdxTime;
    b:=ATime+AdxTime;
    Mx:=(a+b)/2;
    Sigma:=(b-a)/2*sqrt(3);
   end;
1: begin              // экспоненциальный закон распределения чисел в интервале [a,b]
    Sigma:=AdxTime*2;
    a:=ATime-AdxTime;
    b:=ATime+AdxTime;
    Mx:=ATime;
   end;
end;  // end case
AllTime:=-1;
AllCount:=0;
AllZayavkaRun:=0;
for i:=1 to 255 do
 begin
  NextTimeRun[i]:=0;
  KanalStatus[i]:=false;
  KanalTime[i]:=-1;
  KanalCount[i]:=0;
  ZayavkaRun[i]:=0;
 end;
Kanal:=0;
RunParam:=0;
ErrorLevel:=0;
END;
///
// ВЫППОНИТЬ
FUNCTION TKanal.Run:boolean;
BEGIN
Run:=false;
if RunParam=0 then exit;    {если рабочих каналов нет, то выход}
{проверка на освобождение канала}
for i:=1 to MaxKanal do
 begin
  if (GlobalTime=NextTimeRun[i])and KanalStatus[i] then
   begin
    Run:=true;
    KanalN:=i;
    inc(ZayavkaRun[i]);
    inc(AllZayavkaRun);
    KanalStatus[i]:=false;
```

```
    NextTimeRun[i]:=0;
    ZayavkaOut;
    exit;                {выход, необходимо повторить функцию пока Run=true}
   end;
 end;
if WithNakopitel then N.Run; {если есть накопитель, то путь работает}
inc(AllTime);
for i:=1 to MaxKanal do
 begin
  if KanalStatus[i] then inc(KanalTime[i]);  {время вперед}
  {проверка на ошибку}
  if (GlobalTime>NextTimeRun[i])and KanalStatus[i] then
   begin
    ErrorLevel:=3;               //заявка не освободила канал в нужный момент
   end;
 end;
END;
///
// НОМЕР СВОБОДНОГО КАНАЛА
FUNCTION TKanal.GetFreeKanal:byte;
var i:byte;
BEGIN
if Kanal>MaxKanal then
 begin
  ErrorLevel:=4;   // переполнение канала
  exit;
 end;
ErrorLevel:=1;     // возможна ошибка в занятии не свободного канала
for i:=1 to Kanal do if KanalStatus[i]=false then
 begin
  ErrorLevel:=0;   // все в порядке
  GetFreeKanal:=i;
  break;
 end;
END;
///
// УСТАНОВКА СЛЕДУЮЩЕГО МОМЕНТА ВЫПОЛНЕНИЯ
PROCEDURE TKanal.SetNextTime;
BEGIN
KanalNFree:=GetFreeKanal;
repeat
case Zakon of
0: NextTimeRun[KanalNFree]:=round(Normal(Mx,Sigma));
1: NextTimeRun[KanalNFree]:=round(Exponent(Mx,Sigma));
end;  // end case
until (NextTimeRun[KanalNFree]>=a)and(NextTimeRun[KanalNFree]<=b);
NextTimeRun[KanalNFree]:=NextTimeRun[KanalNFree]+GlobalTime+1;
KanalStatus[KanalNFree]:=true;
inc(KanalCount[KanalNFree]);
inc(AllCount);
END;
///
```

```
// ПОСТУПЕНИЕ ЗАЯВКИ В КАНАЛ
// FromNakopitel=true если заявка может поступить только из накопителя,
// false - если поступает новая заявка или заявка из накопителя
PROCEDURE TKanal.ZayavkaIn(const FromNakopitel:boolean);
BEGIN
KanalFromNakopitel:=false;
InNakopitel:=false;
InKanal:=false;{только с накопителя, если есть не пустой накопитель и если есть место в канале,
 тогда заявка поступает из накопителя в канал                    }
if FromNakopitel and WithNakopitel and(N.RunParam<>0)and(RunParam<2) then
 begin  {из накопителя в канал}
  KanalFromNakopitel:=true;
  N.ZayavkaOut;
  inc(Kanal);
  SetNextTime;
  if Kanal=MaxKanal then RunParam:=2 else RunParam:=1;
  exit;
 end;
if FromNakopitel then exit;
{поступление заявки в канал из накопителя или из-вне}
{если есть накопитель и свободен канал и накопитель не пустой, тогда
 заявка из накопителя поступает в канал, а пришедшая заявка поступает в накопитель}
if WithNakopitel and(RunParam<2)and(N.RunParam<>0) then
 begin{из накопителя в канал}
  KanalFromNakopitel:=true;
  N.ZayavkaOut;
  inc(Kanal);
  SetNextTime;
  if Kanal=MaxKanal then RunParam:=2 else RunParam:=1; {пришедшая в накопитель}
  InNakopitel:=N.ZayavkaIn;
  exit;
 end;
{если есть накопитель и свободен канал и накопитель пустой, тогда
 пришедшая заявка поступает в канал                    }
if WithNakopitel and(RunParam<2)and(N.RunParam=0) then
 begin {пришедшая заявка сразу в канал}
  InKanal:=true;
  inc(Kanal);
  SetNextTime;
  if Kanal=MaxKanal then RunParam:=2 else RunParam:=1;
  exit;
 end;{если есть накопитель и канал занят, тогда заявка отправляется в накопитель    }
if WithNakopitel and(RunParam=2) then
 begin
  {канал занят, заявка в накопитель}
  InNakopitel:=N.ZayavkaIn;
  exit;
 end;{если нет накопителя и свободен канал, тогда заявка поступает в канал         }
if (WithNakopitel=false)and(RunParam<2) then
 begin
  InKanal:=true;
  inc(Kanal);
```

```
  SetNextTime;
  if Kanal=MaxKanal then RunParam:=2 else RunParam:=1;
 end;{если нет накопителя и канал занят, тогда выход                    }
END;
///

// УХОД ЗАЯВКИ ИЗ КАНАЛА
PROCEDURE TKanal.ZayavkaOut;
BEGIN
if Kanal-1>=0 then
 begin
  dec(Kanal);
  if Kanal=0 then RunParam:=0 else RunParam:=1;
 end else ErrorLevel:=2; // уничтожение не существующей заявки
END;
///
end.

{модуль выполняющий функции НАКОПИТЕЛЯ}
unit UnitNakopitel;
interface
type
  TNakopitel = class
  Name:string;                  // имя объекта
  AllTime,AllCount:longint; // общее время работы объекта и кол.поступивших заявок
  Emkost,MaxEmkost,             // заявок в накопителе сейчас, макс. возможно заявок
  EmkostMaximum:longint;    // максимально заявок было за время моделирования
  ZayavkaRun:longint;             // количество заявок вышедших из накопителя
  RunParam:byte;                // 0-накопитель полностью пуст
                            // 1-накопитель не пуст и есть место для след. заявки
                            // 2-нокопитель полон, места нет
  ErrorLevel:byte;              // 0-нет ошибок
  PROCEDURE Init(const AName:string;AMaxEmkost:longint);
  PROCEDURE Run;
  FUNCTION ZayavkaIn:boolean;
  PROCEDURE ZayavkaOut;
  end;
implementation
uses main;
// ИНИЦИАЛИЗАЦИЯ
PROCEDURE TNakopitel.Init(const AName:string;AMaxEmkost:longint);
BEGIN
Name:=AName;
AllTime:=0;
AllCount:=0;
Emkost:=0;
MaxEmkost:=AMaxEmkost;
RunParam:=0;
ZayavkaRun:=0;
ErrorLevel:=0;
EmkostMaximum:=0;
END;
```

```
// ВЫПОНИТЬ
{алгоритм
1. Если есть заявка в накопителе, по подсчет статистики }
PROCEDURE TNakopitel.Run;
BEGIN
{1.}
if Emkost>0 then inc(AllTime);
END;
// ПОСТУПЕНИЕ ЗАЯВКИ В НАКОПИТЕЛЬ
FUNCTION TNakopitel.ZayavkaIn:boolean;
BEGIN
ZayavkaIn:=false;
if Emkost+1<=MaxEmkost then
 begin
  ZayavkaIn:=true;
  inc(Emkost);
  inc(AllCount);
  if Emkost>EmkostMaximum then EmkostMaximum:=Emkost;
 end;
if Emkost+1<=MaxEmkost then RunParam:=1 else  RunParam:=2;
END;
// УХОД ЗАЯВКИ ИЗ НАКОПИТЕЛЯ
PROCEDURE TNakopitel.ZayavkaOut;
BEGIN
if Emkost-1>=0 then
 begin
  inc(ZayavkaRun);
  dec(Emkost);
  if Emkost=0 then RunParam:=0 else RunParam:=1;
 end else ErrorLevel:=2;  // уничтожение не существующей заявки
END;
///
end.
```

2) Антагонистік ойын негізінде қашықтықтан оқыту жүйесінің киберқауіпсіздік контурларын құру нұсқаларын оңтайландыруға арналған «Matrix_2020» бағдарламасының m-файлдар листингі

```
//---------------ДОМИНИПРОВАНИЕ ПО СТРОКАМ---------
procedure tform2.optR(Var a1: matrix; var n1, m1:integer; var flag:boolean);
label start;
var i1, j1,k : integer;
//del:array[1..100] of integer;

begin
flag:=false;
start:
 for k:=1 to n1 do
    begin;
    for i1:=1 to n1 do
      begin
        for j1:=1 to m1 do
        begin
          if a1[k,j1]>a1[i1,j1] then break;
          if (k<>i1) and (j1=m1) then
          begin
             form2.DelR(a1,n1,m1,k); inc(pn);flag:=true; goto start;
          end;
        end;
      end;

    end;
end;

//---------------ДОМИНИРОВАНИЕ СТОЛБЦОВ---------
procedure tform2.optS(Var a1: matrix; var n1, m1:integer;var flag:boolean);
label start;
var i1, j1,k : integer;
//del:array[1..100] of integer;
begin
flag:=false;
start:
 for k:=1 to m1 do
    begin;
    for j1:=1 to m1 do
      begin
        for i1:=1 to n1 do
        begin
          if a1[i1,k]<a1[i1,j1] then break;
          if (k<>j1) and (i1=n1) then
          begin
             form2.DelS(a1,n1,m1,k);
             inc(qm);
             flag:=true; goto start;
          end;
        end;
```

```
      end;
    end;
end;
Procedure tform2.DelR(Var X : matrix; Var nn, mm : integer; k1 : integer);
Var
  ii, jj : integer;
Begin
  for ii := k1 to nn+pn do
    for jj := 1 to mm+qm+1 do
      X[ii, jj] := X[ii+1, jj];
        //for jj := 1 to mm do
          //X[nn, jj] := 0;
  Dec(nn);
End;
//----------DELETEs------------
Procedure tform2.DelS(Var X : matrix; Var nn, mm : integer; k1 : integer);
Var
  ii, jj : integer;
Begin
  for jj := k1 to mm+qm do
    for ii := 1 to nn+pn+1 do
      X[ii, jj] := X[ii, jj+1];
        //for ii := 1 to nn do
         // X[nn, jj] := 0;
  Dec(mm);
End;
procedure tform2.minimax();
begin
with form2 do
  begin
SG.RowCount:=SG.rowCount+1;
SG.colCount:=SG.colCount+1;
sg.Cells[SG.colCount-1,0]:='minA';
sg.Cells[0,SG.RowCount-1]:='maxB';
for i:=1 to n do
  begin
    min:=a[i,1];
    for j:=1 to m do
      begin
         if a[i,j]<min then
         min:=a[i,j];
      end;
    a[i,m+1]:=min;
    SG.Cells[SG.colcount-1,i]:=floattostr(min);
  end;
  min:=a[1,m+1];
  mini:=1;
  for i:=1 to n do
      if min<a[i,m+1] then  begin
                            min:=a[i,m+1];
                            mini:=i;
                           end;
```

```
for j:=1 to m do
  begin
    max:=a[1,j];
    for i:=1 to n do
      begin
        if a[i,j]>max then
        max:=a[i,j];
      end;
    a[n+1,j]:=max;
    SG.Cells[j,SG.rowcount-1]:=floattostr(max);
  end;
  maxj:=1;
  max:=a[n+1,1];
  for j:=1 to m do
      if max>a[n+1,j] then begin
                           max:=a[n+1,j];
                           maxj:=j;
                          end;
  end;
end;
procedure TForm2.Button2Click(Sender: TObject);
begin
randomize;
for i:=1 to sg.RowCount-1 do
    for j:=1 to sg.ColCount-1 do
    sg.Cells[j,i]:=floattostr((random(100)-50)/8);
end;
procedure TForm2.UpDown1Click(Sender: TObject; Button: TUDBtnType);
begin
edit1.Text:=inttostr(updown1.Position);
end;
procedure TForm2.Dsimpl;
var i0, j0 : integer;
    tmp : double;
    opt : boolean;
begin
    opt := false;
    repeat
        j0 := 1; i0 := 0;
        while (j0 < m+n+1) and (Ad[m+1, j0] >= 0) do inc(j0);
        if Ad[m+1, j0] >= 0 then opt := true;
        if not opt then begin
            tmp := 10000;
            for i := 1 to m do
                if (Ad[i, j0] > 0) and (Ad[i, m+n+1] / Ad[i, j0] < tmp) then
                begin
                    tmp := Ad[i, m+n+1] / Ad[i, j0]; i0 := i
                end;
            // i0 - выводим, j0 - добавляем
            basis[i0] := j0;                    //добавление нового элемента в базис
            // [i0, j0] -
            for i := 1 to m + 1 do
```

```
                if i <> i0 then
                begin
                    tmp := Ad[i, j0];
                    for j := 1 to m + n + 1 do
                        Ad[i,j] := Ad[i,j] - Ad[i0,j]*tmp/Ad[i0,j0];
                end;
            tmp := Ad[i0, j0];
            for j := 1 to m + n + 1 do
                Ad[i0, j] := Ad[i0, j] / tmp;
        end;
    until opt;
end
//---------------------------
procedure tform2.simplm;
var tk:integer;
begin
    for i := 1 to n do
      for j := 1 to m do
        ad[i,j]:=a[i,j];
    tk:=n;
    n:=m;
    m:=tk;
    for i := 1 to n do fun[i]:=1;     //Заполняем z
    for i := 1 to m do
        Ad[i, n+m+1]:=1;
    for i := 1 to m do
        Ad[i, n+i] := 1;
    fillchar(Ad[m+1], sizeof(Ad[m+1]), 0);
// базис
    for i := 1 to m do
        basis[i] := n + i;
    for j := 1 to n do
        Ad[m+1,j] := -fun[j];            // для не базисных = -fun[j], для базисных - 0

    form2.Dsimpl;                        // DO IT! +)
// -- базис --
    for i := 1 to m+5 do
        if basis[i] <= n then
            xx[basis[i]] := Ad[i, m+n+1];
    for j := 1 to n+5 do
        //if basis[i] <= n then
            yy[j] := Ad[m+1, n+j];
    v:=exp(-1*ln(Ad[m+1, m+n+1]));//-minA;
    tk:=n;
    n:=m;
    m:=tk;
end;
procedure TForm2.Edit1Change(Sender: TObject);
var x:integer;
begin
x:=strtoint(edit1.Text);
sg.RowCount:=x+1;
```

```
for i:=1 to SG.RowCount do
sg.Cells[0,i]:='A'+IntToStr(i);
end;
procedure TForm2.Edit2Change(Sender: TObject);
var x:integer;
begin
x:=strtoint(edit2.Text);
sg.colCount:=x+1;
for i:=1 to SG.colCount do
sg.Cells[i,0]:='B'+IntToStr(i);
end;
procedure TForm2.FormCreate(Sender: TObject);
begin
form2.Edit1Change(application);
  form2.Edit2Change(application);
end;
procedure TForm2.Button3Click(Sender: TObject);
begin
with Sg do
 for i:=0 to ColCount-1 do
     Cols[i].Clear;
for i:=1 to n+m+2 do
  for j:=1 to m+m+2 do
ad[i,j]:=0;
  form2.Edit1Change(application);
  form2.Edit2Change(application);
listbox1.Width:=361;
listbox1.Clear;
for i:=0 to 100 do
  for j:=0 to 100  do
      ad[i,j]:=0;
end;
procedure TForm2.FormKeyPress(Sender: TObject; var Key: Char);
begin
if not (Key in ['0'..'9'] + ['-',',']) then Key:=#0;
end;
end.
```